CENTER for Supply Chain Studies™

ReferenceModel-based Exploration and Education

The Drug Supply Chain Security Act and Blockchain

A White Paper for Stakeholders in the Pharmaceutical Supply Chain

June 21, 2018

www.C4SCS.org

Table of Contents

Contributors

The Center recognizes and thanks the following Study team members and supporters:

Jeff Denton, *AmerisourceBergen*
Heather Zenk, *AmerisourceBergen*
Aditi Kumar, *Amgen*
Donald Rolph, *Amgen*
Miguel Pitarch, *Bristol-Myers Squibb*
Sanjay Sabhlok, *Bristol-Myers Squibb*
Priya Viswanathan, *Bristol-Myers Squibb*
John Dittman, *Cardinal Health*
Jeff Falardeau, *Cardinal Health*
Maryann Nelson, *Cardinal Health*
Dharmesh Patel, *Cardinal Health*
Brian Waeltz, *Cardinal Health*
Robert Celeste, *Center for Supply Chain Studies*
Beth Cusack, *Center for Supply Chain Studies*
Eric Garvin, *Chronicled*
Maurizio Greco, *Chronicled*
Mark Karhoff, *Chronicled (now Genentech)*
Ryan Orr, *Chronicled*
Randy Schwemmin, *Chronicled*
Susanne Sommerville, *Chronicled*
Sam Radocchia, *Chronicled*
Roger Saumure, *Dyadis LLC*
Jerry Castellanos, *Fonterra Co-operative Group*
Dr. Mark Harrison
Justine Freisleben, *Healthcare Distribution Alliance*
Kevin Capatch, *Geisinger*
Dean Parry, *Geisinger*
Martin Braure de Calignon, *GHX*
Steve Cochran, *GHX*
Karen Conway, *GHX*
Peter Knuth, *GHX*
Peter Nelson, *GHX*
Denise Odenkirk, *GHX*
Mark Wilcox, *GHX*
Gena Morgan, *GS1*
Kevin Dean, *GS1 Canada*
Arthur Smith, *GS1 Canada*
Gary Hartley, *GS1 New Zealand*
Tim Mackey, *Global Health Policy Institute*
Maria Palombini, *Inst. of Electrical & Electronics Engineers*
Jim Bracken, *Jim Bracken & Associates*
John Howells, *John Howells Consultant LLC*
Darryl Glover, iSolve
Kasia Piskorska, *iSolve*
Carlos Sanchez, *iSolve*
Gordon Tampol, *iSolve*
Brian Driess, *Johnson & Johnson*
John Melen, *Johnson & Johnson*
Thomas Pizzuto, *Johnson & Johnson*
Christopher Reed, *Johnson & Johnson*
Michael Rose, *Johnson & Johnson*
R. Wilson, *Johnson & Johnson*
John Danese, *KPIT*
Amit Hanamakkanavar, *KPIT*
Hemant Pande, KPIT
Shirish Patwardhan, *KPIT*
Priti Ranadive, *KPIT*
Javid Sayed, *KPIT*
Kevan MacKenzie, *McKesson*
Scott Mooney, *McKesson*
Patrick Andries, *Merck*
Andrei Capitanu, *Merck*
Srinivasarangan *Krishnaswamy, Merck*
Brian McKay, *Merck*
Miroslav Obeslo, *Merck*
David Redanauer, *Merck*
Roman Skultety, *Merck*
Ehsan Ahmadi, *Ohio University*
Glenn MacKenzie, *Pfizer*
Michael Mazur, *Pfizer*
Joseph Pinto, *Pfizer*
Andrew Schmitt, *Pfizer*
Jeff Stollman, *Rocky Mountain Technical Marketing*
Mark Paxton, *Rx-360*
Dagen Wilhelm, *Rx-360*
Claire Cordeaux, *SIMUL8*
Joseph Lipari, *Systech*
Dirk Rodgers, *Systech*
Brian Daleiden, *Tracelink*
Elizabeth Waldorf, *Tracelink*
Ken Traub, *Ken Traub Consulting*
Camille Diges, *Unisys*
Mehdi Entezari, *Unisys*
Kannan Iyer, *Unisys*
John Lillwitz, *Unisys*
Jeff Livingstone, *Unisys*
Dr. Mary Lacity, *University of Missouri*
Jason Geyen, *Verify Brand*
Michael Angelastro, *US Dept. of Health & Human Svcs.*
Patrick Byrne, *US Dept. of Health & Human Svcs.*
Geoffrey Glauser, *US Dept. of Health & Human Svcs.*
Stephen Corma, *US Dept. of Veteran's Affairs*
Marian Daum, *US Dept. of Veteran's Affairs*
Geoffrey Kimber, *US Dept. of Veteran's Affairs*
William Homa, *Walgreens*
Tony Walsh, *Tony Walsh Consultants*

In Memoriam:
Ken Traub

Introduction

The 2013 Drug Supply Chain Security Act (DSCSA) prescribes a set of compliance requirements for pharmaceutical supply chain participants over a ten-year period (2013-2023). Most notably, it requires manufactures of pharmaceutical products sold in the U.S. to serialize, or uniquely identify, pharmaceutical products at the lowest saleable level. Additionally, all supply chain participants must share certain product, production, trading partner and ownership change data.

Of importance to the industry is that in 2023, "interoperable, electronic tracing of product at the package level requirements shall go into effect".[1] Some have interpreted this to mean supply chain participants are required to put in place an **electronic system to facilitate the collection of information** for all current and previous changes of ownership (*leading back to the original manufacturer or repackager*).

Specifically, the DSCSA calls for:

- Exchange of Transaction Information (TI) and Transaction Statement (TS)
- Systems and processes for verification of product at the package level
- Systems and processes necessary to promptly respond with the TI and TS information
- Systems and processes necessary to promptly facilitate the gathering of information to produce the TI going back to the manufacturer
- Ability to only accept saleable returns for products that they can associate to the TI and TS

There are concerns that retrieving TI data back to the manufacturer could require tens of thousands of electronic connections between previously "unconnected" participants. Essentially, each supply chain participant might need to form an electronic connection with each potential company participating in their supply chain. *Currently, no such electronic system exists.*

Blockchain technology has demonstrated a strength in creating a single source of truth that is highly resistant to corruption – either accidental or intentional. It also holds promise for being able to restrict access to competitively valuable transaction data only to those parties with a defined "need to know," providing the confidentiality sought by trading partners.

Current blockchain platforms offer an environment of simplified electronic connections between parties for data distribution, synchronization and immutability, programmability, visibility, security and potentially, confidentiality – all characteristics of an effective environment where trading partners can enforce business and regulatory rules and securely automate the exchange of data. *(It should be noted that the language of the DSCSA calls for transaction data exchange to be interoperable. In some quarters this is seen as being different than an interoperable system.)*

In this highly complex and regulated industry,
the Study Team explored if blockchain technology can be used
to address the full data sharing requirements of the DSCSA.

[1] H.R. 3204 Title II – Drug Supply Chain Security Act: Sec. 203. (g) Enhanced Drug Distribution Security

DSCSA and Blockchain Study

Overview

This white paper provides insights into the team's process, exploration and learnings throughout the Study. Future teams will build upon the learnings of this group and take the next steps of building proof of technology, proof of concept, pilots and extensions on the basic DSCSA data set used in this work.

Building the team, setting the goals.

In the winter of 2017, a group of regulatory, operations, clinical, I.T. and other backgrounds from 50 healthcare industry stakeholder companies and associations came together as a team to explore the use of blockchain technology to support Drug Supply Chain Security Act (DSCSA) compliance and to add additional value.

Considering the requirements of the DSCSA and the current state of data sharing in the industry, the team established a list of goals to address during the study that were considered important for the industry to be able to support DSCSA compliance in 2019 and 2023.

The list included:

- Establishing an electronic connection between non-adjacent trading partners
- Establishing trust between these trading partners
- Sharing required data without inadvertently exposing proprietary information
- Reducing the potential activity required of trading partners
- Designing for expansion beyond DSCSA compliance
- Funding the architecture
- Reducing risk

Together, the team established a framework for holding exploratory discussions (described later in this paper). This outline structure allowed the team to consider governance, technology, services and supply chain practices clearly and distinguish between DSCSA requirements, supply chain needs and individual trading partner pair agreements. Initial talks served to establish a level of knowledge among team members on the complex topics of the DSCSA, supply chain practices and blockchain technology.

Next, we created various exploratory designs (or models) in which these three complex topics might be brought together to aid in DSCSA compliance and adding additional value. These designs were cast into simulated ReferenceModels™[2] to enable the team to exercise some of the data sharing rules and explore potential data outputs.

[2] ReferenceModels™ are key to the Center's Study process. They are computer simulations and diagrams of the supply chain and supply chain stakeholder interactions that explore various design alternatives, regulation interpretations, future states and technology usage. They also help Study teams to animate, test and evaluate a current or proposed scenario.

The U.S. Pharmaceutical Supply Chain

The role of the trading partners.

Like most of today's mature supply chains, the U.S. pharmaceutical supply chain contains many types of trading partners, as well as the companies who support them with logistical and data services solutions.

Trading partners are highly controlled by various regulatory bodies and certifying agencies. Caution must be taken when contemplating any type of change as new requirements may impact existing regulatory or certification rules. Often, in our discussions of DSCSA-related process changes, stakeholders advised us of existing requirements that needed to be taken into consideration.

An example of this is the DSCSA requirement that a trading partner cannot receive product without also receiving proper DSCSA mandated information. In the case of a temperature sensitive drug, for instance, there are also requirements that the drug be placed in a temperature-controlled environment to maintain the efficacy of the drug.

Defining the Study parameters.

These and many other requirements lead to further conversations on the accuracy of process and data definition to avoid conflicting with one rule while attempting to comply with another. The Design Models discussions helped clarify current and proposed process controls and practices and explore the impact of laws, regulations and technology on the supply chain and individual trading partners.

The team tackled new challenges as it worked through DSCSA definitions and requirements of supply chain participant types and the (sometimes) multiple roles that the trading partners perform. To clearly address these issues and allow for typical supply chain behavior and individual trading partner agreements, the team assigned ReferenceModel rules into these three categories:

1. **DSCSA:** The rule can be directly linked to language in the DSCSA
2. **Supply Chain:** The rule exists due to established practices and trading partner needs
3. **Trading Partner Agreements:** Recognizing that trading partners can choose to share additional data based on their individual business arrangements

Defining these rules allowed the team to have targeted, exploratory discussions on several topics without blurring the lines between what is specifically called for in the law and what may be desired or needed by trading partners. They also helped us in establishing ReferenceModel runs that tested whether data created in a trading partner to trading partner agreement can successfully be held confidentially in the shared industry blockchain.

The Drug Supply Chain Security Act[3]

The Drug Supply Chain Security Act (DSCSA) contains a vast array of requirements to be implemented over a ten-year period (2013-2023). The Study concentrated on requirements that the supply chain must comply with by the year 2023 and all previous requirements that will still be in effect then.

Specifically, the team focused on a scenario where all required finished drug products are serialized (are marked with a 2D barcode containing the NDC (GTIN), Serial Number, Lot Number and Expiration Date), trading partners are required to share Transaction Information (TI) and Transaction Statement (TS) and where trading partners have *"The systems and processes necessary to promptly facilitate gathering the information necessary to produce the transaction information for each transaction going back to the manufacturer, as applicable."*

When the law was drafted, there were expectations that all DSCSA defined data would be included in a single "document". The Study team took the point-of-view of a trading partner – able to collect all the data from appropriate sources and coalesce the data into a "document" if needed. This strategy falls within existing master data management practices and efficient storage practices.[4]

A note on the DSCSA Transaction Statement:

The Transaction Statement is a series of attestations that the transferring trading partners are required to make to those trading partners with whom the product is being sent. These include confirmations that the product was purchased directly from the manufacturer, exclusive distributor of the manufacturer, or repackager that purchased the product directly from the manufacturer when that purchase occurred. Trading partners have been making these attestations either by including the specific language of the DSCSA or by reference. In February 2018, the FDA issued a Draft Guidance allowing for a shortened attestation.

All ReferenceModels developed by the Study Team assume that a shortened attestation would be allowed and that further, an automated means of attestation may be allowed. This could be an indicator in the TI data set could be set, or an attestation that any post to the system would constitute attestation that the posting body has complied with the language in the law. As a result, the ReferenceModels described in this white paper do not address Transaction Statement requirements.

[3] https://www.fda.gov/drugs/drugsafety/drugintegrityandsupplychainsecurity/drugsupplychainsecurityact/default.htm

[4] See Center's Study on DSCSA and MDM: https://c4scs.org/s/White-Paper-DSCSA_MDM_Center-for-Supply-Chain-Studies_FINAL.pdf

Blockchain Technology

Wikipedia defines blockchain as:

"A **blockchain**, originally **block chain**, is a continuously growing list of records (Figure 1), called *blocks*, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority."

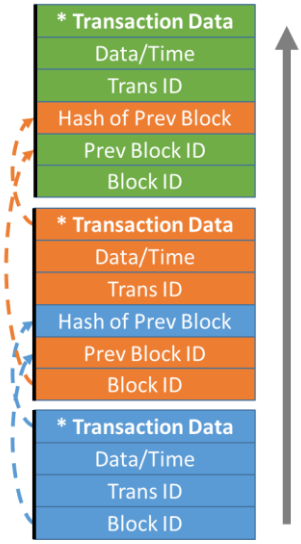

Figure 1: *Blockchain*

Key observations of blockchains

- By design, inherently resistant to modifications of data *(data is said to be immutable)*
- They are utilities upon which business applications can be built
- They distribute data securely and ensure all copies are identical
- Each process may be assessed a fee *(may be key to funding industry shared blockchains and as a deterrent to nefarious activity)*
- They are programmable using distributed applications (DApps), sometimes known as Smart Contracts *(could be used to enforce industry and regulatory rules)*
- The DApps are also visible, immutable and distributed
- Correctly developed DApps can be verified and their output predicted and trusted

Many blockchain platforms[5] incorporate the concepts of blockchain and additional capabilities based on the types of uses anticipated. For the purposes of this Study, we did not assume the use of any one. Instead, we explored and simulated the capabilities available in many popular platforms:

- Data is "write only" *(cannot be changed or deleted once posted to the blockchain)*
- Data may be visible to all parties connected to the blockchain
- Full copies of the blockchain data may be distributed to all blockchain nodes
- Distributed applications *(which trading partner systems can interact with)* can access and act on data stored on the blockchain
- Distributed applications can enforce data access and certain data quality rules *(such as data format)*
- Use of special applications (oracles) that can access information that resides outside (off) the blockchain

[5] Article on different blockchain platforms: https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

The team also explored and discussed features that are implemented in a few blockchain platforms and are envisioned to be available in the future, including:

- Substantial data storage located off the blockchain, yet accessible to the blockchain and distributed applications on the blockchain
- Indexing of blockchain data to enable querying and retrieval
- Data obfuscation *(blockchain platform features to obfuscate data and retain query features)*

Standards usage

Unique Identification, Data Attribution, Process Controls, Labeling and other standards are foundational to sharing data and provide the ability to simplify business transactions, improve efficiencies and reduce risk. They allow innovations to be accepted and incorporated into existing practices with the least amount of overhead or customization. All ReferenceModels created in this Study make use of appropriate standards such as identification, transaction, data and process.

Specifically, the ReferenceModels made use of these standards:

GS1 Identifiers

- Global Trade Item Number (GTIN)
- Serialized Global Trade Item Number (SGTIN)[6]
- Lot Global Trade Item Number (LGTIN) [7]
- Serial Shipping Container Code (SSCC)
- Electronic Product Code (EPC)

GS1 Traceability Standards

- Electronic Product Code Information Services (EPCIS)
- Core Business Vocabulary (CBV)
- Tag Data Standard (TDS)

GS1 Data Definitions

- Global Data Dictionary

GS1 US DSCSA related attributes and EPCIS usage

- GS1 US Implementation Guideline: Applying GS1 Standards for DSCSA and Traceability

[6] GS1 Tag Data Standard version 1.9: The SGTIN is a EPC URI syntax and is composed of a GTIN and a serial number

[7] GS1 Tag Data Standard version 1.9: The LGTIN is a EPC Class URI syntax and is composed of a GTIN and a Lot Number

Concepts

Industry-Shared Blockchain (ISB)

Although some individual solution providers may use a blockchain platform for their service, the Industry Shared Blockchain (ISB) refers to the platform(s) that connects all individual services. The Distributed Logic in the ISB is the result of industry stakeholder consensus and is available for those stakeholders to validate.

Connecting to the blockchain through a Service Provider

A supply chain participant looking to establish an electronic connection with others would first register with a service connected to the ISB. That service will ensure the company is assigned a proper identity on the blockchain and fulfills its obligations in terms of initial setup such as identification of products and establishment of them on the ISB *(for ReferenceModels where this is required).*

Confidentiality

A process by which data is only shared with appropriate trading partners. Regarding DSCSA, this means that each trading partner should be able to access Transaction Information (TI) for items they have or are about to take ownership of. They should be able to access TI for the exchange in which ownership is transferred to them and all previous transfers within the supply chain. Trading partners should not have access to TI of items or shipments for which they never had ownership. Exceptions to this rule are 3PLs who do not take ownership but are required to have access to TI for shipments of which they previously had custody.

Scenarios

Although there are many nuanced scenarios that take place within the supply chain during the life cycle of a pharmaceutical product, these are the scenarios discussed throughout the study to determine the potential role of blockchain technology.

Transfer of product between trading partners

In this basic scenario, items are transferred from one trading partner to another without error. Party 1 commissions and packages the items and ships to Party 2. Party 2 receives the items, verifies that the items received were placed into commerce by the manufacturer (commissioning took place) and prepares them for the next step (storage, unpacking and repacking for shipment, dispensing). A series of trading partners can be linked together to vary the scenario.

Saleable return

The receiving trading partner (Party 2) returns product to the sender (Party 1). Party 1 verifies that ownership of the returned item was originally transferred from Party 1 to Party 2. Party 1 also verifies that the items were placed into commerce by the manufacturer and that there is no other information to indicate that the items should not be treated as saleable product.

Non-saleable return

The receiving trading partner (Party 2) returns product to the sender (Party 1). Party 1 verifies that ownership of the returned item was originally transferred from Party 1 to Party 2. Party 1 also verifies that the items were placed into commerce.

In this scenario, Party 1 finds the items are not saleable (expired, recalled, damaged, etc.). Party 1 then either returns the items to the party they received them from (manufacturer or another wholesaler) or transfers them to a Returns Processor (Party 3). Party 3 destroys the product and provides information of the destruction to the manufacturer.

Delayed information availability

Items are transferred from one trading partner to another without error. The Manufacturer (Party 1) commissions and packages the items and ships to Party 2. However, Party 1 processes their information in batches and the Transaction Information (TI) becomes available several hours after the shipment arrives at Party 2. Party 2 secures the product, indicates that the TI is not available and processes the items up to the point of shipment or use. Prior to shipment or use, Party 2 must verify that TI from Party 1 is available and that the item was placed into commerce by the manufacturer (commissioned).

Hospital Pharmacy Borrow and Loan

A hospital requires a drug that is either not available or may be costly and seldom used. The hospital arranges to borrow a quantity of the drug from another local hospital. The borrowing hospital may, or may not, know the patient (e.g., a previously admitted patient or a newly arriving patient). The borrowing hospital acquires the drug from the lending hospital and replaces the drug once they acquire new stock of the drug.

Exception processing

Errors do occur. Logistics units are sometimes packed incorrectly, shipments arrive at the wrong destination, etc. Discrepancies between what took place and what was *recorded as taking place* need to be corrected.

A key feature of blockchain technology is data immutability. On most ledgers, entries are corrected by posting offsetting entries. The Study team explored this concept and found that it could lead to misunderstandings when attempting to replay and understand a series of transactions. Instead, it employed a simple “replace” mechanism by indicating that the corrective transaction replaces a previous (erroneous) transaction. This works for most cases and only is an issue when the desired effect is to have a transaction ignored (it was in error, won’t be replaced and needs not to be part of any transaction set analysis). An efficient method of correcting information in an immutable dataset remains a challenge.

Challenges

The Study team explored challenges regarding the complexity of the DSCSA statute and interpretation, the nuances of Supply Chain practices and the ever-evolving blockchain technology and platforms. *A few of the challenges included:*

The Drug Supply Chain Security Act (DSCSA)

Multi-link transactions:

Most transactions (ex: orders, invoices, payments, etc.) in business are [8]between two trading partners. The DSCSA requires *(depending on your interpretation)* sharing certain data with the entire list of trading partners responsible for transferring packages to the dispenser. For the purposes of this Study, transactions were recorded at the smallest saleable package level.

SEC. 203(g)(1)(E) of the DSCSA:

Retrieving previous Transaction Information going back to the manufacturer. *For example*: in Figure 1 below, the hospital may be required to retrieve TI^1 and TI^2. These transactions contain data (ship dates, quantities, etc.) that is confidential between the transacting trading partners. For the purposes of this Study, confidential data from previous transactions were redacted or removed when shared with trading partners who were not parties to the transaction.

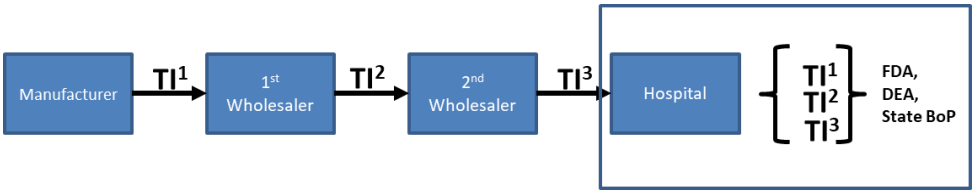

Figure 2:
Transaction Information sharing

2019, Verification of saleable returns:

Beginning in November 2019, the DSCSA requires wholesalers to verify that the manufacturer placed the Product Identifier (PI)[9] in commerce for packages returned that the wholesaler determines are saleable. This is a challenge to the wholesalers as, by this date, packages will be marked with the Product Identifier. However, manufacturers are not required to transmit the product identifiers in the TI until November 2023.

The result is the need for a system that enables wholesalers to request verification of the PI and for manufacturers to provide verification. This system may not be needed in 2023 when manufacturers will begin to pass the PI in the TI and wholesalers will have the information to verify saleable returns.

[8] https://www.fda.gov/drugs/drugsafety/drugintegrityandsupplychainsecurity/drugsupplychainsecurityact/default.htm

[9] The DSCSA defines the Product Identifier as the National Drug Code (NDC), Serial Number, Lot Number and Expiration Date. In practice, the NDC is imbedded in a Global Trade Item Number (GTIN), a product identification standard of the GS1 standards body.

The Supply Chain

Multiple company identifiers:

The DSCSA requires that TI and TS be shared between trading partners upon the change of ownership. Changes in product location (i.e. a change of custody) may not always cause a change in ownership in activities such as intra-company transfers or transfers using a third-party logistics provider (3PL), and do not require TI and TS to be shared.

Study scenarios were constructed under the assumption that companies will use their corporate identification to document change of ownership. However, some States require transacting companies to be licensed in the State. This may require an implementation where one (corporate) blockchain account ID be associated with more than one transacting entity ID to correctly discern transactions that were made between divisions of the same company and between separate trading partners. Incorporating the use of company hierarchy repositories such as GS1 Global Location Number repositories could support this distinction between federal and state law.

Data access governance:

Who sees what data when? This is partially addressed in the DSCSA statute itself. Typical transactions (orders, invoices, ship notices, etc.) pass between two trading partners. In the DSCSA requirements, certain data is passed serially from one trading partner to another. Lot numbers, expiration dates, etc., make up the Transaction Information (TI) that each trading partner must make available to their customers.

Ensuring that TI data is accessible to only those in the supply chain that have, or have had, ownership of the package may require a choreography of digital signature exchange, clever encryption and or other methods being investigated such as zero knowledge proofs[10].

Blockchain

Obfuscating data on the Blockchain:

As data on most of today's blockchain platforms is visible to all connected parties, it is necessary to obfuscate confidential data stored on the blockchain. Also, as the DSCSA is a traceability-only law, prior trading partners should not be able to un-obfuscate data authored by future trading partners. In the end, there is very little if any data that can remain un-obfuscated on the blockchain.

Confidentiality can be attained in several ways:

1. Access to the data can be limited by rules that are hard coded into the blockchain software and that are implemented in rigidly enforced operational processes.
2. The data itself can be encrypted and the decryption keys carefully managed to limit its use to approved parties. Unfortunately, encrypted data becomes difficult to query.

[10] A **zero-knowledge proof** or protocol allows a "prover" to assure a "verifier" that they have knowledge of a secret or statement without revealing the secret itself.

3. Various obfuscation techniques can be employed that obscure certain data items (notably, the identify of trading partners) without limiting the ability of approved parties to selectively query the database.

4. A data architecture can be crafted that keeps humans from seeing the data once it has been validated by the transacting parties. Maintenance of the blockchain consensus can be maintained by machines without intervention (other than independent auditing). The information that is required to be passed on can be generated by reports. *This fourth option was not investigated in the Study.*

The team experimented with a few mechanisms to obfuscate the data including encrypting the data[11], digitally signing[12], storing only hash values and zero knowledge proofs as a mechanism to protect data. Encryption and signing introduce additional steps of exchanging keys and key management into the overall data exchange and storage process.

We found that encryption of the product and trading partner identifiers itself was not enough to protect against parties who might examine large volumes of transactions, often looking for and matching patterns to aid in discerning who the trading partners were or what the product being transferred was.

We then explored using the full PI (GTIN, Serial Number, Lot Number and Expiration Date) to create enough differentiation and rely on the barcode as the mechanism to transfer knowledge of the PI. This produced a less "guessable" encryption. However, this encrypted value would also be identifiable for each transaction in which the item occurred. The need for an additional data value that changed with each transaction created an encrypted value that was not repeated across transactions. This also produced data that was not searchable by legitimate trading partners.

Though unrefined, a few of the mechanisms were able to adequately obfuscate the data. The overall opinion of the team was that this is a critical link to the future success of blockchain. The team also agreed that blockchain platforms, developers and cryptographers are now developing effective mechanisms that can provide efficient methods to protect sensitive data from prying eyes and to search for and share data among trading partners.

Data storage limitations:

As ledgers of transactions, blockchain platforms are not currently designed to efficiently store, index and retrieve vast amounts of data. This challenge is worked around in some blockchain applications by using near-block data storage solutions such as IPFS[13], Oraclize[14], IOTA[15], BigchainDB[16] and other services.

Also, some blockchain platforms are addressing the storage issue by incorporating data storage services or forming connectivity with existing data storage platforms (*ie.: Ethereum and IFPS*).

[11] When encrypting, you use **the reader's public key** to write message and the reader uses **their private key** to read it.
[12] When signing, you use **your private key** to write message's signature, and the reader uses **your public key** to check if it's really yours.
[13] IPFS: Interplanetary File System, a protocol and network designed to create a method of storing and sharing hypermedia in a distributed file system., https://ipfs.io/
[14] Oraclize: data-transport-layer for blockchain. www.oraclize.it/
[15] IOTA: designed to be the data layer for the internet of things. https://www.iota.org/
[16] BigchainDB: Database with blockchain characteristics, https://www.bigchaindb.com/

Multiple platforms:

Several blockchain platforms are currently in use and under development. They are being created as solutions in both the public domain and as in the private sector. As it is doubtful that one single platform solution will eventually be used across all industries, a key challenge is how the blockchain ledger concept and its programmability can be extended across platforms.

Many organizations are actively exploring ways for blockchain platforms to interoperate.

Cost:

Funding an industry-wide platform is a daunting challenge at best. However, there are many ways to fund such a solution including fees for memberships, volume-based subscriptions and transactions.

Costs fall into three categories:

1. Cost of building, deploying, maintaining and supporting the shared blockchain infrastructure
2. Cost of building, deploying, maintaining and supporting company-unique infrastructure *(e.g., local repositories including access control and help desks as well as adapters to feed the shared infrastructure)*
3. Cost of inefficiency *(incurred by trading partners trying to access local repositories and needed to recall username/password or work with the help desk of the repository owner)*

Many blockchain platforms have a built-in mechanism for supporting the transaction fee model to pay for the processing, connectivity and necessary data storage. Blockchain platforms use an electronic token or currency required for each transaction to fund the organizations that support the network.

Posting a transaction on a blockchain requires a fee for each process executed. Fees are paid from the account of the user much like how *E-Z*Pass deducts a fee every time you drive over a toll bridge. This provides an automated incentive for those companies supporting the operation of the platform and reduces processing fees for the companies that use the platform.

A volume-based subscription fee model could support pricing tiers based on volume. Firms would pay a fixed-price per month, based on their annual volume tier. The advantage of this model is that by offering fixed pricing, it makes it easier for firms to budget.

An underlying transaction fee or token model could be used by service providers to share fees based on usage. The automated models that are native to many blockchain platforms may be a bit of a culture change for corporations that are used to more traditional payment models.

ReferenceModels: **DSCSA and Blockchain**

Simulating the environment

A simulated environment allows teams to go beyond diagrams and to test certain hypotheses. Simulation is akin to building a prototype of real world and computerized systems and sheds insight into potential business changes by animating process, information and cash flows. It provides a virtual view into how regulatory interpretation and company policy affect trading partner behavior and helps to uncover details that may be overlooked when using diagrams alone to assess impact of change on a business environment.

Several scenarios discussed by the team were simulated throughout the course of the Study. The results of those simulations and the data they generated – referred to as ReferenceModels™ – were then shared and verified with the team.

The ReferenceModels depict existing processes in the supply chain and allowed the team to experiment with various strategies for using blockchain technology to support DSCSA requirements. After experimenting with many strategies, we settled on three (3) main ReferenceModels that incorporated different strategies for using blockchain technology to share, archive and evaluate the DSCSA Transaction Information (TI). Each model contains unique characteristics that affect the manner of sharing and the type of processing that each trading partner is responsible for to support the model.

The three models are:

- ReferenceModel™ 1

  Store full TI in an industry-shared blockchain platform for retrieval. Also, transact EPCIS events directly between trading partners to communicate the contents of shipments and logistics units.

- ReferenceModel™ 2

  Store addresses or pointers to trading partner portals or repositories of TI for retrieval in an industry-shared blockchain platform. Also, transact EPCIS events directly between trading partners to communicate the contents of shipments and logistics units.

- ReferenceModel™ 3

  Send DSCSA TI to blockchain platform distributed applications (DApps) that evaluate the data and store current "states" of the individual Product identifier. An expanded version includes shipment hierarchy and may alleviate the need to transact EPCIS events directly between trading partners.

A note on the ReferenceModels:

This was an exploratory Study. The ReferenceModels were used to provide some level of analysis of the outcome of Study team hypothesis. The ReferenceModels and all associated process flow and data model diagrams should be viewed in context of experimentation and not as finished, implementable artifacts. Some experiments continued until the team gained a specific insight and were not worked through to completion. Even though the data models use Entity Relationship Diagram notation, the relationships between data sets are for illustration purposes only. For instance, all models include data that is extracted from EPCIS events. The relationship between the Product Master dataset and the ObserveEvent dataset is an example of a suggested relationship. It is meant to suggest that the ProductID (in the form of a GTIN) in the Product Master dataset can be found in the EPC List of SGTINs in the EPC List. This relationship cannot be directly deployed in a database and only suggests that there is in fact, a relationship.

Establishing the Study framework

To aid in the exploration, the team established a framework (*see* ***Figure 3***) for discussing and understanding the interrelationships between the supply chain participants (supply chain sub-model), services (services sub-model) that may provide access to the blockchain and provide access to off-blockchain data, the blockchain and distributed network (data persistence sub-model) and the governance body (governance sub-model) which might be the gatekeeper to a private, permissioned blockchain platform, determine consensus data access rules and oversee the management of the system.

Core to keeping a clear distinction between what is necessary for DSCSA compliance, supply chain operations and potential trading partner to trading partner agreements, the team adopted three categories of design rules:

1. **DSCSA:** The rule can be directly linked to language in the DSCSA
2. **Supply Chain:** The rule exists due to established practices and trading partner needs
3. **Trading Partner Agreements:** Recognizing that trading partners can choose to share additional data based on their individual business arrangements

Defining these rules (categories) allowed the team to have targeted, exploratory discussions on several topics without blurring the lines between what is specifically called for in the law and what may be desired or needed by trading partners. Additionally, they helped in establishing ReferenceModel runs that tested whether data created in a trading partner to trading partner agreement can successfully be held confidentially in the shared industry blockchain.

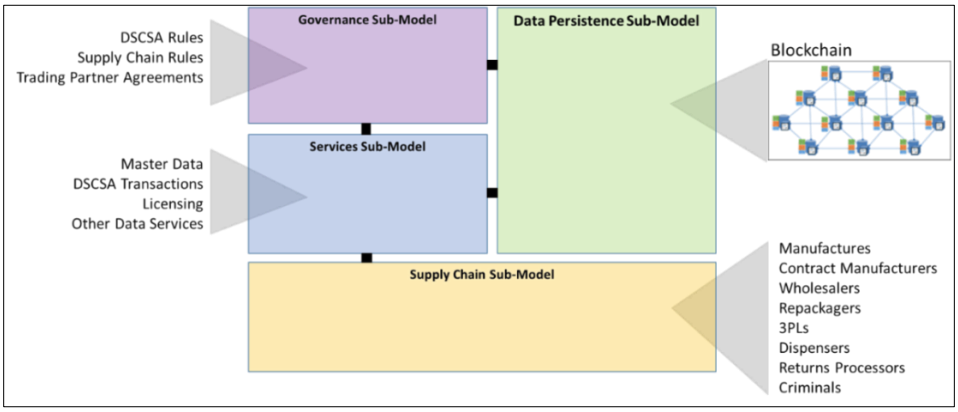

Figure 3:
Framework for Exploring Complexities

Although the team explored many avenues for using blockchain technology to support DSCSA requirements, we defined three models as alternatives. There were many variations within each model to accommodate different interpretations of the statute, governance issues, trading partner requirements and blockchain platform differences. The three ReferenceModels described here represent the major design alternatives that the team explored along with commentary from the team on their assessment of the models. We do not claim that they exhaustively represent the full range of possible solutions.

ReferenceModel 1:
Transaction Information Ledger

Definition

As shown in Figure 4, this model specifies that the data attributes of the DSCSA defined Transaction Information (TI) and Transaction Statement (TS) be stored in or, adjacent but accessible, to the blockchain platform. The initial version of this model specified that the TI attributes be stored in a blockchain transaction in an obfuscated manner. Currently, blockchain platforms are not designed to efficiently store, encrypt and retrieve large amounts of data. Most blockchain platforms extract a premium for storing data over a set limit. Encrypting and otherwise masking data must be accomplished prior to posting the data on the blockchain.

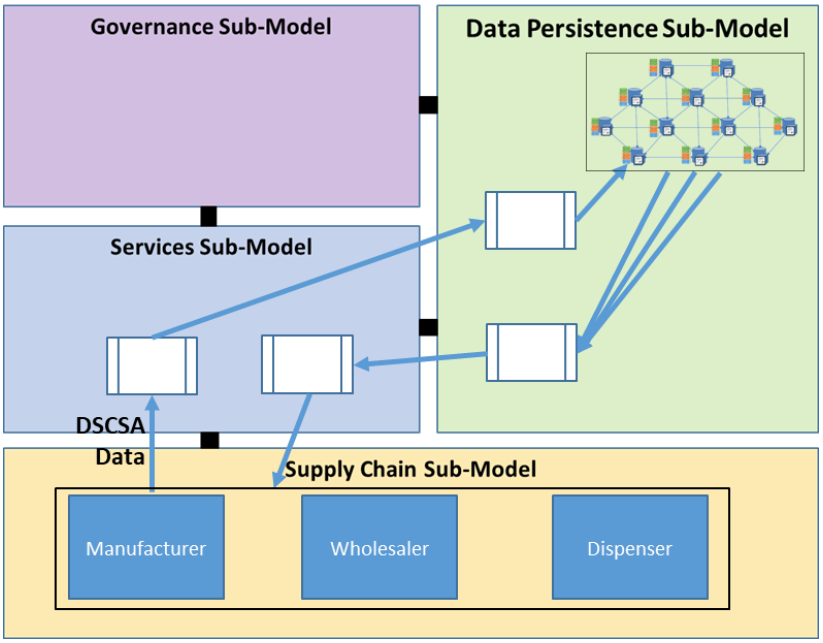

Figure 4:
ReferenceModel 1 – *TI/TS on the blockchain*

In ReferenceModel 1 (**Figure 4**), supply chain trading partners provide TI data to a service provider via a specified subset of GS1 EPCIS events. The provider (*provides access to the blockchain*) extracts essential data attributes from the EPCIS event and calls a distributed application (DApp), or other programs, on the blockchain platform established to process the event type.

The DApp checks to see if this trading partner is permissioned to post the type of event and if so, posts the event to the blockchain ledger. When event data are required, the trading partner sends an EPCIS Query Event to their service provider. The service provider's system calls the appropriate query DApp on the blockchain, which checks whether the trading partner has permission to the data. If so, the blockchain DApp retrieves the data and sends the data to the service provider who formats the data into an EPCIS Query response and sends it to the trading partner.

Assumptions

- Private, permissioned blockchain[17]
- GS1 Identifiers used for products, logistics units and parties
- Data on blockchain is encrypted or hashed
- Use of on blockchain programming (distributed applications, or DApps) to control posting and querying
- URI format of identifiers is used (SGTIN, GLN, SSCC, etc.)
- Use of EPCIS Event and Query data
- Use of EPCIS EventID to reference events
- Use of EPCIS standard "ErrorDeclaration" to indicate that an event identified by the EventID is voided
- Correcting Events must be posted for events declared in error

Feature observations

Governance:

As all DSCSA data is stored on the blockchain, it is most likely that the effort of governance will be high. All supply chain stakeholders posting data will, most likely, want representation during data visibility rule making (who gets to see what, under what circumstances). Implementation of the rules and validation of the programming code will also be complex.

Operations:

Each supply chain stakeholder (or their proxy) will be responsible for retrieving EPCIS Event data sets and evaluating them to make their own determination of actions. Evaluating data sets for each item under control (pallets, cases, totes, units) can cost resources and time.

Risk:

As each stakeholder evaluates the data available to them separately, this could lead to trading partners arriving at different conclusions about compliance. *For example, trading partners have their own policies as to whether a receiving event is necessary in acknowledgement of a shipping event*[18].

Cost:

High governance and operational costs.

Compliance:

Letter of DSCSA Law:

- *SEC. 203(g)(1)(A): "The transaction information and the transaction statements as required under this section shall be exchanged "*
- *SEC. 203(g)(1)(E): "facilitate gathering the information necessary to produce the transaction information for each transaction going back to the manufacturer"*
- ReferenceModel 1A fulfills letter of the law in that it includes all DSCSA data in one post and is accessible for retrieval

[17] Private, permissioned blockchain platforms allow industries to choose high performing network nodes and set and enforce criteria or rules for companies to access the blockchain.

[18] Relates to the use of GS1 EPCIS events and not blockchain itself.

- ReferenceModel 1B recognizes that trading partners exchange product master data and party master data prior to an order being executed (current best practice). This model assumes the trading partners already are in possession of product, customer and supplier master data and doesn't include it on the blockchain.

Intent of DSCSA Law:

ReferenceModel 1A and 1B could be regarded as both meeting the intent of the law. 1B provides additional efficiencies by adhering to master data management best practices.

Supply chain integrity:

Counterfeits:

As all DSCSA data is on the blockchain, it is possible to detect both a fake SNI and a fraudulent second commissioning of a legitimate SNI. Evaluation of packing and shipping events could detect duplication of an item.

Theft and reentry:

ReferenceModel 1 allows for "Recall" events to be posted. It may be possible to alert holders of items identified in a Recall event.

Exception management:

EPCIS contains an "Error Declaration" element that can be used to indicate that an EPCIS event is in error and identify the replacing event.

SWOT analysis:

Strengths:

1. Simple design complies with DSCSA requirements
2. DSCSA TI data is kept together as a record of truth at a specific point in time. Changes to trading partner and product information do not affect the data recorded at the time of the blockchain transaction.

Weaknesses:

1. Obfuscating data and making it accessible and interpretable by the correct parties is an issue with this and all models.
2. Currently, data must be obfuscated prior to posting to the blockchain, making it difficult to look up needed data. A mechanism outside of the blockchain must be used to share keys and indicate which transaction applies to each shipment which re-introduces the requirement of establishing an electronic connection with many trading partners (*a main reason for blockchain exploration*).

   A possible alternative might be to assign a set of identities with random addresses (like randomized serial numbers), making it hard to correlate all the different packages that a trading partner is shipping. But, the information does not require decrypting. Instead, some control node (possibly controlled by the trading partner) can correlate the source of the packages when needed. This is like a manufacturer maintaining a list of commissioned serialized packages.

3. Massively duplicated product and party master data (data about the product, supplier or customer). Product and party master data are typically acquired prior to an order. As the DSCSA includes a 2023 requirement[19] to gather previous TI information, this means that data either needs to be stored at the DSCSA defined package level (package level granularity), or via sophisticated algorithms to trace back through the various logistic units, a package has been part of in its lifetime.

   In the case of package level granularity, product and party master data would be duplicated for each package produced. This would increase data storage requirements, cost and risk of data errors.

Opportunities:

1. If obfuscation and on-block data storage challenges are resolved, the TI information could be normalized[20] and stored efficiently on a blockchain (*see ReferenceModel 3 below*).
2. There are "add on" services that can augment blockchain storage or provide blockchain benefits in a platform that can also manage large quantities of data efficiently (ie: BigchainDB, IPFS, etc.). These services can provide a link in the blockchain transaction to the actual data. Groups are actively working on integrating storage capacity services that can meet the industry's performance needs.
3. Private, permissioned blockchains can be configured to accommodate data sets relatively economically due to the option of specifying performance metric meeting network nodes.
4. Links to off-block sources or the use of blockchain oracle technology could be added to expand the use of this data beyond DSCSA compliance.

Threats:

1. Obfuscating billons of blockchain transactions could result in a large "key management" issue for trading partners. Managing keys may be a larger challenge than managing the DSCSA data itself for small trading partners.
2. Loss of keys could disrupt product flow while key exchange is established manually.

Observations:

1. Posting the entire TI on the blockchain as one large transaction rather than posting it in logical groupings makes the data more difficult to use for purposes other than DSCSA compliance. Product and Party master data should not be repeated for each transaction. The idea of normalizing the data and posting data groups in separate transactions would mimic how data is stored in databases and could be used or expanded for other purposes. *ReferenceModel 3 expands on this concept.*
2. Because TI data is committed directly to the blockchain and data access rules are established and enforced by DApps, data governance becomes a complicated and costly burden. All companies posting data will want representation when the access rules are established, implemented and verified. This model would enact a large data governance commitment in terms of resources and cost on trading partners.

[19] See "Traceability Requirement" in Appendix. Note: Some parties do not make this same interpretation of the statute. It was used, however, for the purposes of this Study.

[20] Normalization is a process to group like data attributes together, minimizing duplication.

ReferenceModel 1:

Life cycle of a pharmaceutical package

Posting data to the blockchain

Here is an example of the use of ReferenceModel 1 (see Figure 5), where GS1 EPCIS event data is stored directly on the blockchain:

Prior to transacting, the trading partners (*manufacturer, wholesaler and dispenser*) would exchange their blockchain Account ID and possibly public keys (to decrypt posted transactions). A manufacturer would create and hold EPCIS events as product is labeled, packed into cases, cases packed onto pallets and shipped to the purchasing wholesaler. Upon shipping the product to the wholesaler, the manufacturer would post the held EPCIS events (commissioning, packing and shipping) to the blockchain for the packages, cases and pallets shipped. The wholesaler would be alerted to this shipment by one of three possible avenues:

1. An Advanced Shipment Notice
2. Direct EPCIS XML event delivery
3. Alert from a DApp on the blockchain via their blockchain Account ID

The wholesaler would either evaluate the directly delivered EPCIS events (and possibly match them with the blockchain posted data) or retrieve the blockchain posted data and treat it as the one source of truth. This process would be repeated for the transaction between the wholesaler and dispenser as depicted in **Figure 5**.

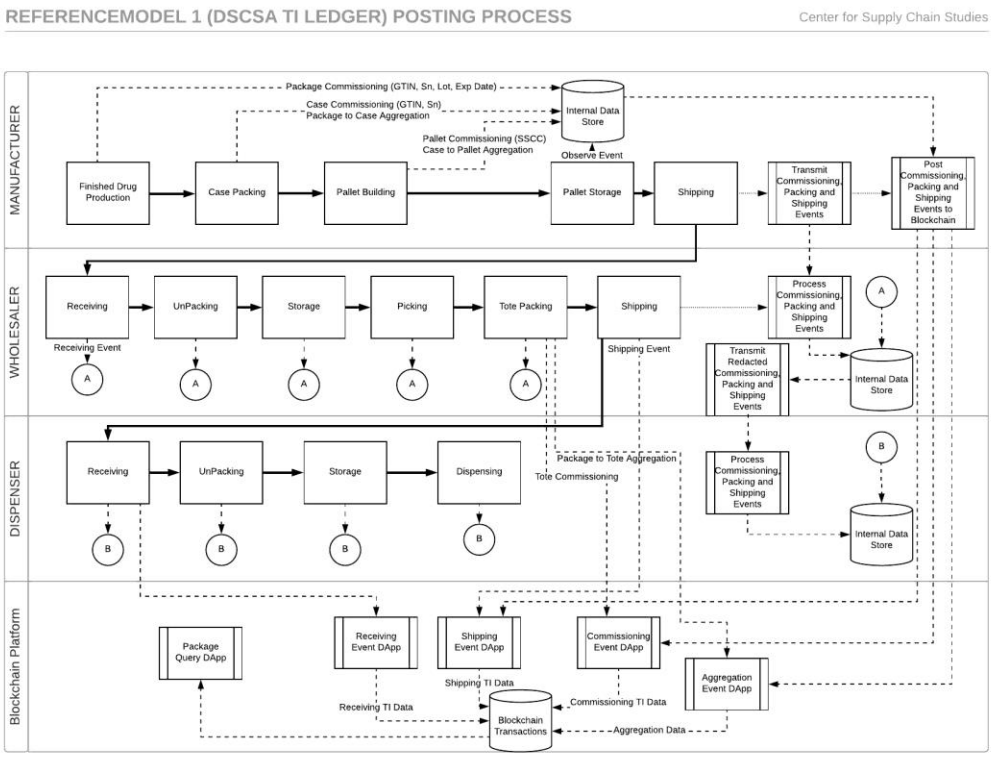

Figure 5:
ReferenceModel 1 – *DSCSA TI data on the blockchain*

ReferenceModel 1:

Verifying the manufacturer place a package into commerce

For any trading partner to verify that a package was placed into commerce, they would need to access the commissioning data that the manufacturer posted or shared. If the commissioning data was shared directly via an GS1 EPCIS commissioning event, the trading partner would know that it was placed in commerce. What they *wouldn't* know is whether anything occurred in the interim that would cause them to not sell, transfer, dispense or administer the product.

Using ReferenceModel 1, the trading partner could query the blockchain to retrieve all transactions they were legitimately allowed (data governance rules) to access. The trading partner would be able to assess whether the manufacturer, or anyone else in the supply chain had posted an event that would render the product unusable (recall, damage, expired, etc.). **Figure 6** diagrams the verification process for the sample wholesaler and dispenser.

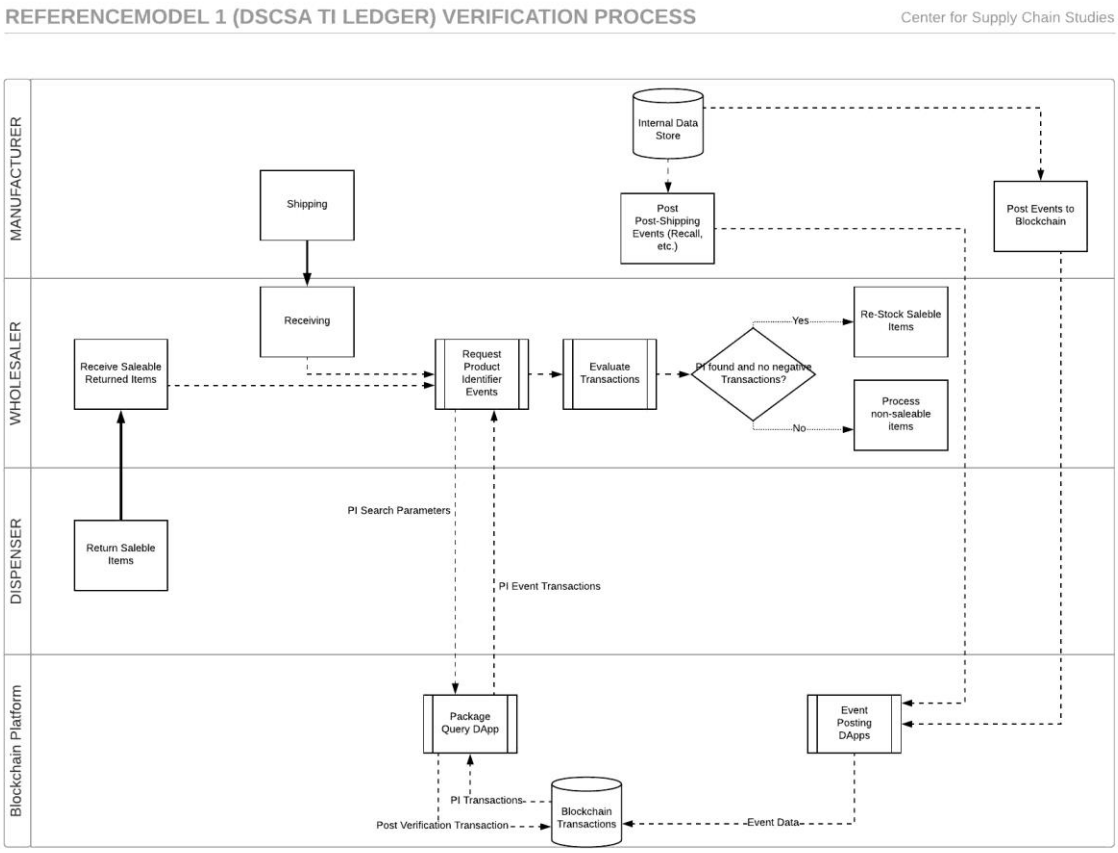

Figure 6:
ReferenceModel 1 – *Verification Process*

ReferenceModel 1:
The Data

The data depicted in **Figure 7** is non-normative and was used to experiment with placing the TI data on the blockchain. It shows the data that each trading partner holds internally and the data that is posted to the blockchain platform.

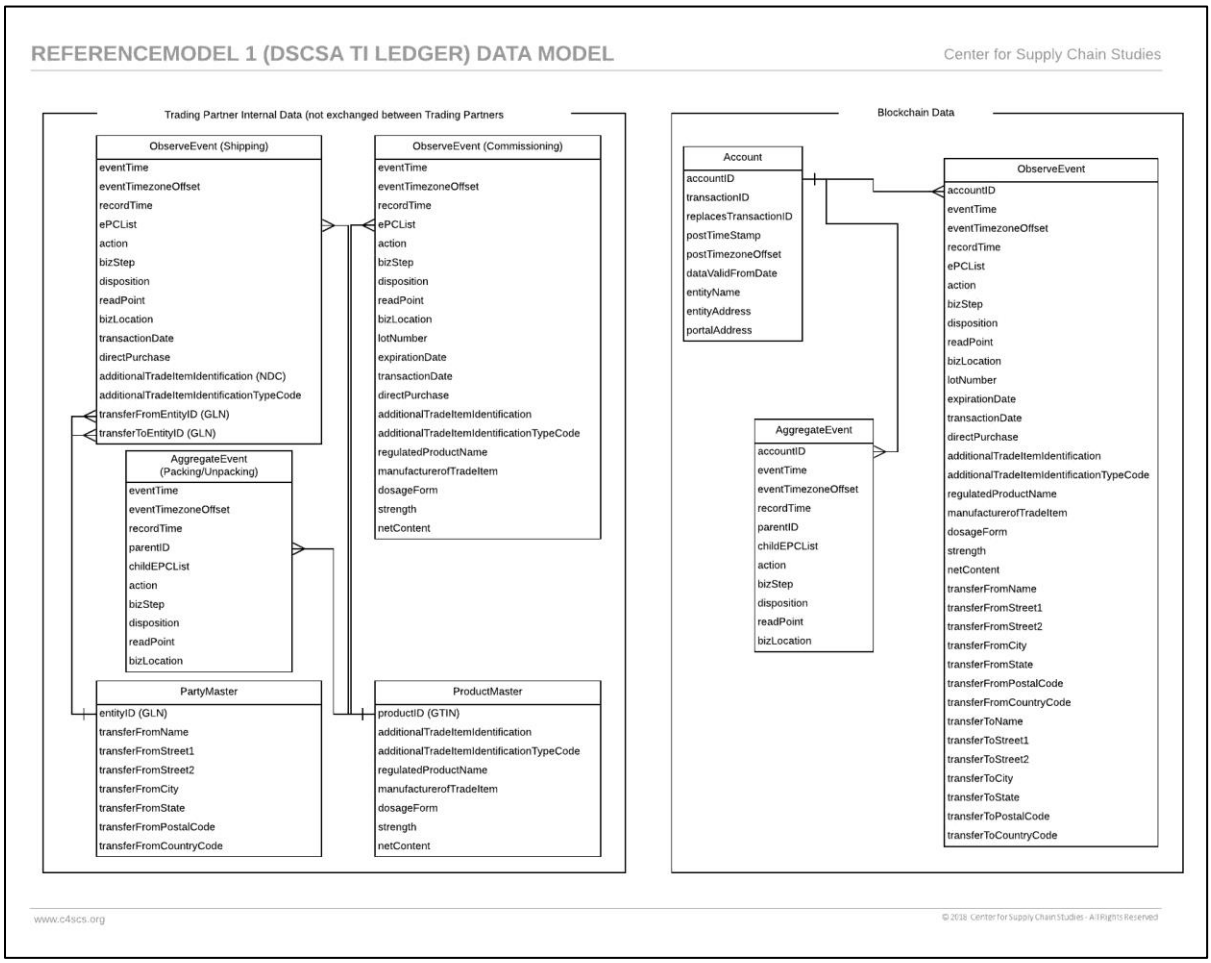

Figure 7:
ReferenceModel 1 – *Trading Partner and Blockchain Data*

ReferenceModel 2:
Directory service

Definition

As shown in **Figure 8**, this model specifies that pointers, or addresses to EPCIS repositories, DSCSA portals or other services be stored in the blockchain. The blockchain would serve as a sort of "directory" of DSCSA and other data. Hash values calculated on original EPCIS events are also posted to the blockchain along with the repository address and can be used later to determine if the retrieved data matches the original data provided by the authoring trading partner.

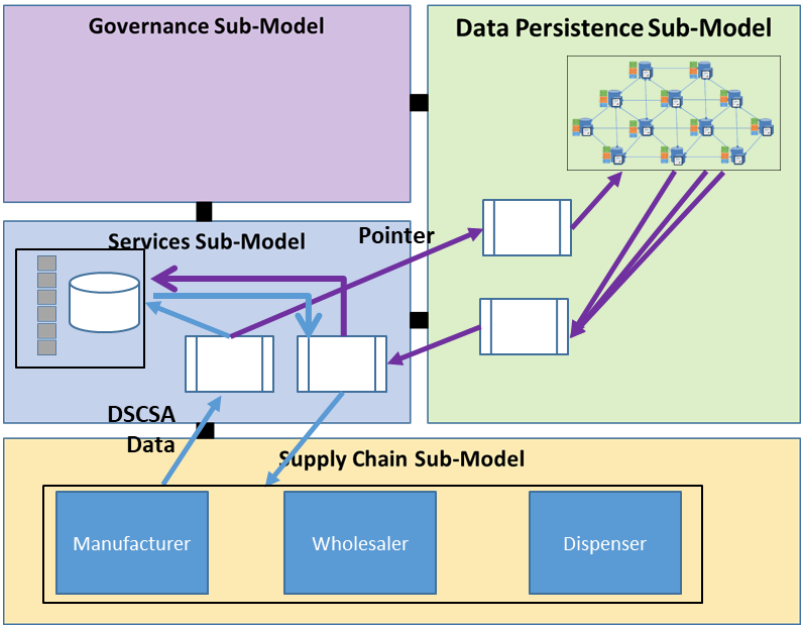

Figure 8:
ReferenceModel 2 – *Directory Service*

In ReferenceModel 2, supply chain trading partners provide TI data to a service provider via GS1 EPCIS events. The service provider stores the events in a repository and calculates a hash value based on the event. The service provider calls a DApp on the blockchain platform established to process the event type. The call includes the hash value and the address established by the service provider where EPCIS queries are accepted and processed. The DApp checks to see if this trading partner is permissioned to post the information and if so, posts information to the blockchain ledger.

When event data are required, the trading partner sends an EPCIS Query Event to their service provider. The service provider's system calls the appropriate query DApp on the blockchain, which checks whether the trading partner has permission to the data. If so, the blockchain DApp retrieves the hash and address of the service provider holding the original event. The trading partner's service provider then queries the data source address and retrieves the EPCIS event data. The hash value can then be checked to ensure the retrieved event data is identical to the event sent by the original trading partner. The service provider then provides the event data to the querying trading partner.

Assumptions

1. Private, permissioned blockchain[21]
2. GS1 Identifiers used for products, logistics units and parties
3. Data on blockchain is encrypted or hashed
4. Use of on blockchain, programming (distributed applications, or DApps) to control posting and querying
5. URN and URI formats of identifiers (SGTIN, GLN, SSCC, etc.) are used
6. Use of EPCIS Event and Query data
7. Use of EPCIS EventID to reference events
8. Use of EPCIS standard "ErrorDeclaration" to indicate that an Event identified by the EventID is voided
9. Correcting Events must be posted for events declared in error

Feature observations

Governance:

As all DSCSA data is stored off the blockchain in private repositories controlled by the supply chain stakeholder or their solution provider. It is most likely that the effort of governance will be low in terms of data access of blockchain data.

Each EPCIS Repository establishes and executes their own data governance rules. There is the potential for disputes if querying parties and queried parties disagree on whether events should be shared or if data elements should be redacted. Implementation of the rules and validation of the programming code will also be complex on an individual EPCIS Repository basis. However, the bulk of governance activity will be in defining standardized data access protocols for individual EPCIS repositories:

1. Standards will need to be developed with which trading partners will need to comply to make their data accessible. This is likely to be a similar effort to defining data standards for keeping all data on the blockchain.
2. Governance will be needed to enforce the standard when a query to a trading partner fails.

In comparing ReferenceModel 1 and 2, the issue shifts from relying on third-party solution providers to preserve the confidentiality of the data on the blockchain to relying on each supply chain partner to control their own data. This will likely require more "governance" and more cost, but it may make executives feel more comfortable with the security of their confidential data.

Operations:

Retrieving EPCIS Event data is a two-step process in ReferenceModel 2.

First the querying party must retrieve the EPCIS Repository address for the object in question, then retrieve the DSCSA data from the addressed EPCIS Repository. This process may repeat itself as it is possible that certain events (Shipping, Receiving) may be accomplished at the outer packing hierarchy level. In that case, the querying party may need to apply an algorithm or series of queries to navigate the packaging hierarchy.

Each supply chain stakeholder (or their proxy) will be responsible for retrieving EPCIS Event data sets and evaluating them to make their own determination of actions. Evaluating data sets for each item under control (pallets, cases, totes, units) can cost resources and time.

[21] Private, permissioned blockchain platforms allow industries to choose high performing network nodes and set and enforce criteria or rules for companies to access the blockchain.

This system also requires that each local repository be available 24x7 to respond to queries that can occur on a 24x7 basis because significant elements of the supply chain operate around the clock. Each repository would then need to provide solution to maintain uptime through both scheduled and unscheduled (emergency) maintenance activities.

Risk:

As each stakeholder evaluates the data available to them separately, there could be issues of trading partners arrive at different conclusions (regarding compliance). Each individual EPCIS Repository may have different response times for returning query results.

Cost:

Lower Governance cost for data stored on the blockchain, however, higher cost in managing data locally and responding to trading partner's queries. Also, due to the added number of processing steps, there may be a higher cost to retrieve data than ReferenceModel 1.

Trading partners will also have to develop governance processes from establishing access control accounts for third-party access to their repositories, as well as help desks to support third parties legitimately accessing data in the repositories.

With a multiplicity of repositories to access – each of which may have difference procedures – trading partners will incur costs in time lost gaining access to repositories and using trading-partner help desks to help them "remember" each company's procedures and logon credentials.

Compliance:

Letter of DSCSA Law:

ReferenceModel 2 fulfills letter of the law in that it includes all DSCSA data in one post available in the queried EPCIS Repositories.

Intent of DSCSA Law:

ReferenceModel 2 could be regarded as meeting the intent of the law, however, there may be difficulty in determining duplicate SNIs.

Supply chain integrity:

Counterfeits:

The Industry blockchain will hold multiple addresses for each item (manufacturer, wholesaler, dispenser, etc.). Only by querying and retrieving DSCSA data from all addresses can an evaluation be made whether there is a single trail back to the manufacturer or multiple. It's not clear what stakeholder might take on that responsibility.

Recalls:

ReferenceModel 2 allows for "Recall" events to be posted. In a pure "repository address only" model, a Recall event would look like any other event unless the EPCIS Repository was queried. An additional mechanism or indicator may be needed on the industry blockchain to more quickly identify recalled items and alert holders of those products.

Exception management:

EPCIS contains an "Error Declaration" element that can be used to indicate that a EPCIS Event is in error and to identify the replacing event.

SWOT analysis:

Strengths:

Data control is guaranteed in that data is held directly by the authoring trading partner or their proxy service provider. Each trading partner can implement their own set of data access requirements and rules.

Weaknesses:

1. Obfuscating data and making it accessible and interpretable by the correct parties is an issue with this and all models.
2. Because TI data is stored in separate repositories, DApps may not be able to detect duplicate PI data. Duplicate PI data may occur because of a data or processing or labeling error or because of counterfeit activity.
3. The number of interfaces and transactions necessary to post to the blockchain and retrieve data is far greater than the other models.
4. For the system to work, there needs to be conformance to norms and performance metrics to keep the solution from becoming needlessly complex and costly.
5. The possibility that a repository is down at a time when it is needed is high, given the large number of repositories required and the high cost of providing 24x7 uptime.
6. Each trading partner would need to manage access control for its repository. This would likely also require providing help-desk service to resolve issues when other trading partners encounter issues accessing the repository.
7. Trading partners seeking to lookup data may have to manage many accounts IDs and passwords to access the various repositories. And because such accesses may be infrequent, outside partners would not memorize the unique access information for each trading-partner repository. They would likely require help-desk support on an ongoing basis.
8. If encryption keys are used to protect the data in a repository, key management may be complex and costly.

Opportunities:

This model can be extended to include links to additional data stores that may valuable for other trading partner processes.

Threats:

Because of the complexity of managing access for hundreds of repositories, there is a high likelihood that some repositories would be vulnerable to attack to gain access to their contents. This could be for reasons of competitive intelligence or more nefarious purposes.

Observations:

The current model is based on a single directory. It may be the case that the directory concept would be implemented in different blockchains. In this case, an additional layer of interoperability between directories would be needed. Interoperating across directories could impact performance, add data governance complexity and add cost or add complexity to service calculations.

ReferenceModel 2:
Life cycle of a pharmaceutical package

Posting data to the blockchain

As an example of the use of ReferenceModel 2, where addresses where GS1 EPCIS event data could be accessed is stored directly on the blockchain. The hash value of the EPCIS event data would also be posted on the blockchain to act as a check once the actual data was retrieved from the trading partner.

Prior to transacting, the trading partners (manufacturer, wholesaler and dispenser) would exchange their blockchain Account ID and possibly public keys (to decrypt posted transactions). A manufacturer would collect EPCIS events as product is labeled, packed into cases, cases packed onto pallets and shipped to the purchasing wholesaler. Upon shipping the product to the wholesaler, the manufacturer would post the address of their EPCIS repository (held by them or their solution provider) along with the hash of each EPCIS event data set. The wholesaler would be alerted to this shipment by one of three possible avenues:

1. An Advanced Shipment Notice
2. Direct EPCIS XML event delivery
3. Alert from a DApp on the blockchain via their blockchain Account ID

In the scenario where the wholesaler did *not* receive the EPCIS event directly, they would query the blockchain for the addresses where EPCIS repositories holding events for the package in question. The wholesaler's system would then query each EPCIS repository and retrieve the available events. The wholesaler would then calculate a hash value for the events and match against the blockchain version of the hash value. Upon matching, the retrieved EPCIS events would be treated as the one source of truth. This process would be repeated for the transaction between the wholesaler and dispenser (depicted in **Figure 9**).

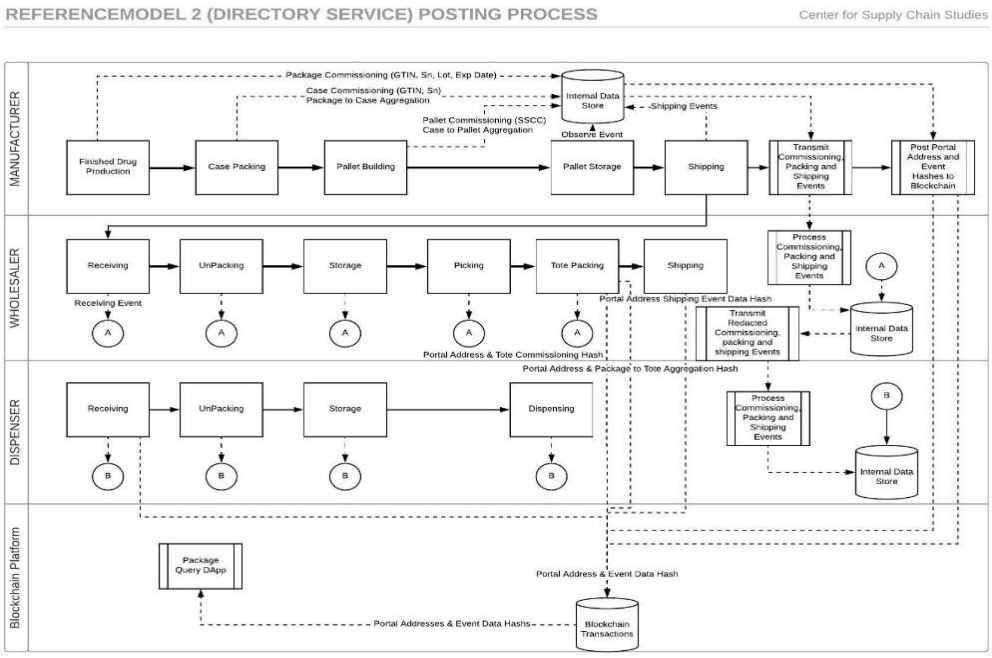

Figure 9:
ReferenceModel 2 – *Directory Service*

Verifying the manufacturer placed a package into commerce

For any trading partner to verify that a package was placed into commerce, they would need to access the commissioning data that the manufacturer holds. The trading partner would repeat the process outlined above of first retrieving the EPCIS repository addresses from the blockchain and then querying those addresses for the commissioning data. The trading partner would know that it was placed in commerce. However, they would *not* know whether anything occurred in the interim that would cause them to not sell, transfer, dispense or administer the product.

This process might be supplemented by a separate "verification" database maintained by the manufacturer to explicitly support verification lookups. But, each manufacturer then would be responsible for ensuring that the query came from someone owning the package in question.

Using ReferenceModel 2, the trading partner could query the blockchain to retrieve all transactions they were legitimately allowed (data governance rules) to access. The trading partner would retrieve those events and evaluate them to determine whether the manufacturer, or anyone else in the supply chain had posted an event that would render the product unusable (recall, damage, expired, etc.). Figure 10 diagrams the verification process for the sample wholesaler and dispenser. (*See **Figure 10**.)*

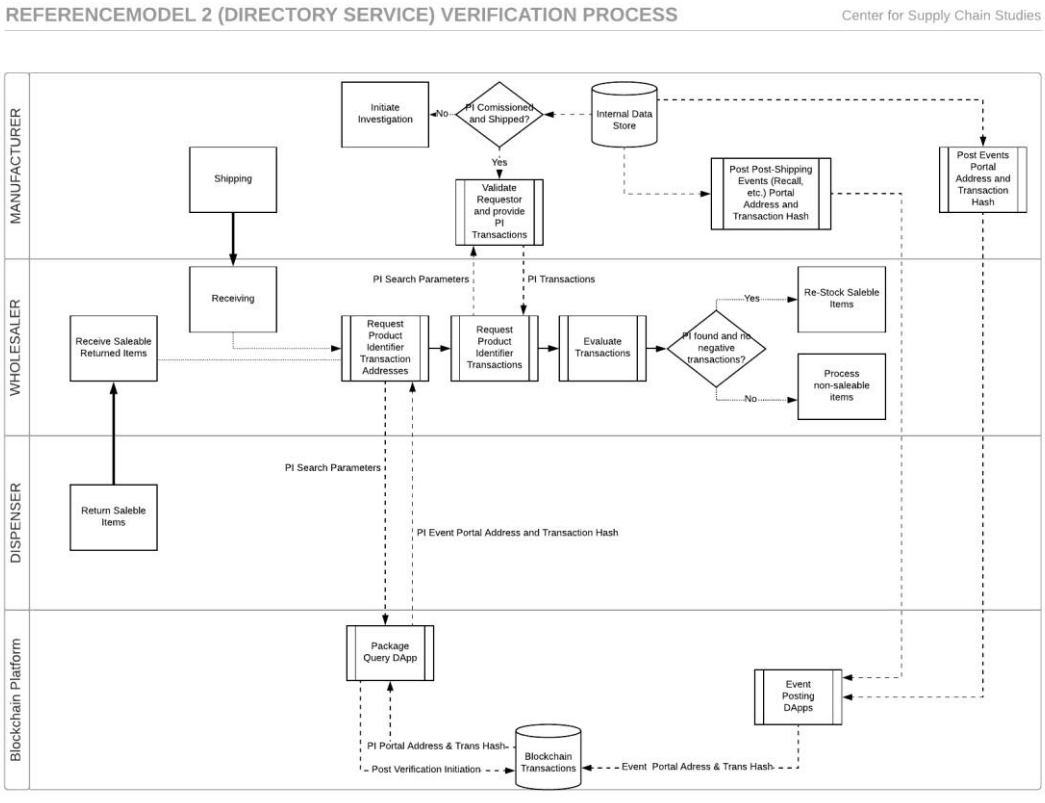

Figure 10:
ReferenceModel™ 2 – *Directory Service Verification*

ReferenceModel 2:
The Data

The data depicted in **Figure 11** is non-normative and was used to experiment with placing the TI data on the blockchain. It shows the data that each trading partner holds internally and the data that is posted to the blockchain platform.

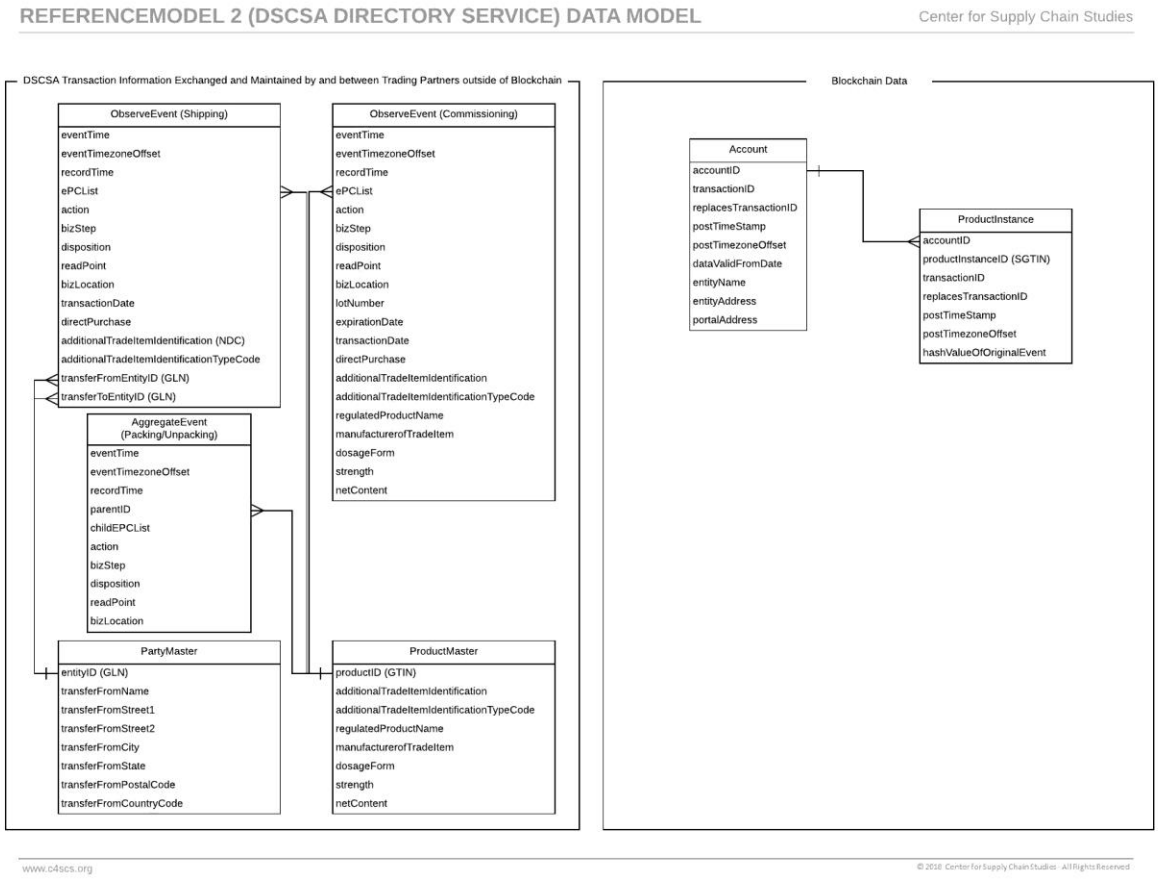

Figure 11:
ReferenceModel 2 – *Trading Partner and Blockchain Data*

ReferenceModel 3:
Product "states"

Definition

This model takes a different approach to DSCSA and operational requirements than in ReferenceModels 1 and 2. Although this model calls for the archival of EPCIS events (for investigation purposes), it only stores a few "states" of the package as it transitions the supply chain. The model relies on *on-blockchain* DApps to interpret incoming EPCIS events, archive them and post only the "state" of the package. The premise is, if DApp code is visible to all, then all can validate that the code would interpret a given set of incoming data (or EPCIS event) and all could trust the "state" that the DApp set based on the incoming data and visible DApp logic. The "states" constitute actionable information, upon which trading partners could make predictable business decisions. *The States we explored were:*

1. **DSCSA product:** ***Does the product fall under the DSCSA?*** Non-DSCSA items in the supply chain will be serialized. It is difficult for downstream trading partners to be aware of which products fall under DSCSA and which do not. This state could save resources in quarantining non-DSCSA product unnecessarily, believing it might be a DSCSA product without the required TI/TS.
2. **Grandfathered:** ***By Nov. 2018, all product that falls under the DSCSA will be serialized.*** However, passing serialized TI is not required until 2023. There will be a period after 2023 where there will exist serialized product without TI and serialized product with TI. The Grandfathered state identifies those products that legitimately do not have associated TI available. These products will all exit the supply chain at some point. At that point, this state will be unnecessary.
3. **Fit for Commerce:** There are many events that would indicate that a package was not fit for commerce (*such as recall, damage, expired product, temperature excursion, determination of illegitimacy, etc.*). If the posting DApp encounters any of these events, it posts a "fit for commerce" state of false. This gives a clear indication to supply chain and clinical operations as to what should be done with the product.
4. **In Commerce:** ***Has the product been placed in commerce by the DSCSA-defined manufacturer?*** This state provides some level of security in that it is not set to "true" until the manufacturer ships or places it into commerce. This state would provide a clear data point for wholesalers attempting to verify saleable returns and inspections involving counterfeit or stolen products.
5. **Provenance:** ***Have the observed transactions regarding a package added up to a clear link back to the manufacturer?*** If an investigation were to take place, would the archived transactions show the series of TI's back to the DSCSA defined manufacturer.
6. **Declared Emergency:** The DSCSA contains provisions where TI and TS sharing can be suspended in the event of a declared emergency. To not render that product illegitimate after an emergency, a manufacturer (*or entity that transferred the product*) must declare which product was part of the emergency. This state provides the mechanism to make that declaration clear to all trading partners that may receive the product in the future.
7. **Declared Emergency ID:** While not a "state," the team experimented with a way to identify the emergency and which authority declared it.

The team explored two alternatives to maintaining the state of the package on a blockchain. The first was to introduce an Internet of Things (IoT) concept by creating an address for each thing (*package*). This was accomplished by creating a DApp for each package using a hashed version of the PI as the name of the DApp (thereby creating a sort of address for each package). The states were maintained in the DApp's allocated memory.

Because DApp deployment on the blockchain is expensive, the second alternative involved exploring a method for posting transactions that list the latest state. While not as IoT-like as the DApp method, it did remove the burden for each subsequent trading partner to accurately evaluate a growing string of events. This method drastically reduced trading partner processing and risk that trading partners of theirs could interpret the events differently. This model also reduces the risk that regulators (FDA, State Boards of Pharmacy, etc.) could interpret a series of events differently than the trading partner.

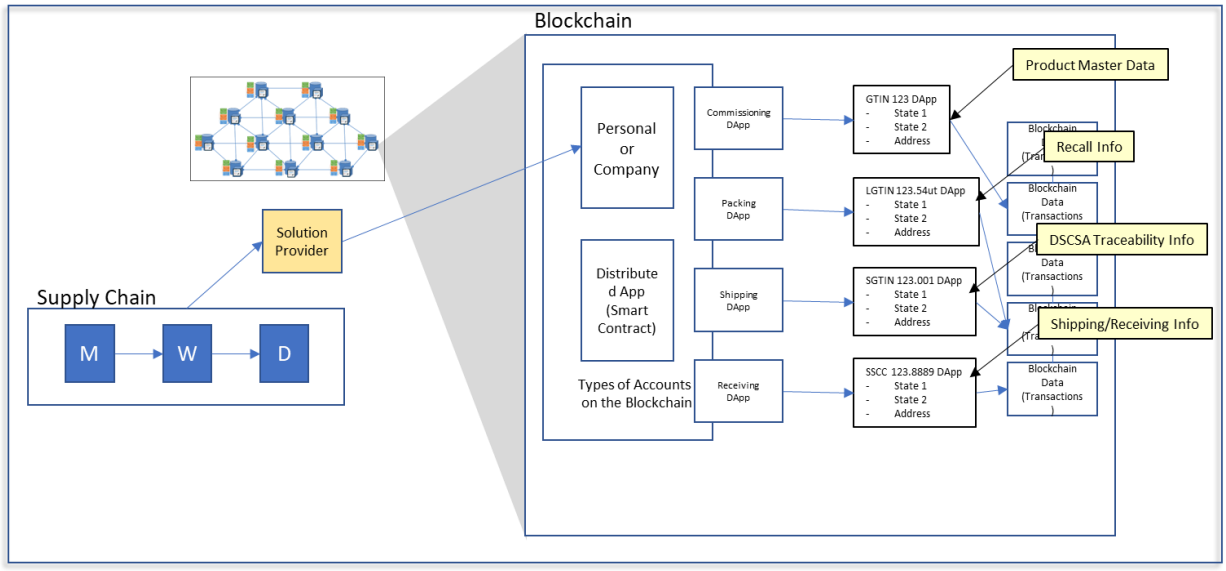

Figure 12:
ReferenceModel 3 – *Product, Lot, Package and Logistics Unit State*

Expanding the value of state management

Links for additional information:

While this model was designed to provide quick answers to pressing question of trading partners, there is also the need to link back to the EPCIS events that were evaluated by the DApps (to determine that state). Therefore, we explored adding a link attribute to the states which allowed for trading partners to retrieve associated events and for entities to provide additional data associated with the product that might be of value beyond DSCSA compliance.

Other "things":

As depicted in **Figure 12**, the concept of maintaining state and links to other information can be expanded to create efficiencies (less duplicate data) and added value for DSCSA and other needs. *They include:*

1. **Product Information:** Identified by a GS1 Global Trade Item Number (GTIN), information about products (master data) can be posted to cover minimum DSCSA needs and links to more, in depth data.
2. **Entity Information:** Trading partners in the models are identified by their GS1 Global Location Number (GLN). Master data about the entity or location can be accessed through a posted link.
3. **Product Lot:** Expiration Date and Lot number are set by the manufacturer for each Lot produced. This and other information about the Lot could be posted here. Recalls typically are at the Lot level. Recall events could set a state at the Lot level advising of the recall and setting a link for more information.
4. **Package:** This level of information has been covered in the basic description above. Each package could have a series of states to reflect the context of the package.
5. **Logistics Units:** Identified by the GS1 Serial Shipping Container Code (SSCC), this set of data could include packaging hierarchy, which is needed for receiving, inference and in the event of selling through sealed manufacturer cases, providing TI to trading partners.

The Transaction Information (TI) defined within the DSCSA law contains data attributes about many levels of product hierarchy and logistics units. Those levels can be identified using GS1 and other standards.

Table 1:
State can be maintained for products, instances, logistic units and locations

Object	Standard ID	Example[22]
Finished Product	GS1 GTIN	urn:epc:id:sgtin:0031234.500012.0
Finished Product Lot Info	GS1 LGTIN	urn:epc:id:lgtin:0031234.500012.201801ABC
Serialized Finished Product	GS1 SGTIN	urn:epc:id:sgtin:0031234.500012.12345
Logistics Unit	GS1 SSCC	urn:epc:id:sscc:0031234.500043.12345678
Entity	GS1 GLN	urn:epc:id:sgln:031234.500001.0
Location	GS1 GLN	urn:epc:id:sgtin:031234.500012.0
Internal Location	GS1 GLN + Extension	urn:epc:id:sgtin:031234.500012.12345
Document	GS1 GDTI	urn:epc:id:gdti:031234.000123.12345

[22] See GS1 Tag Data Standard for explanation of format: https://www.gs1.org/standards/epcrfid-epcis-id-keys/epc-rfid-tds/1-11

Assumptions

1. Private, permissioned blockchain[23]
2. GS1 Identifiers used for products, logistics units and parties
3. Data on blockchain is encrypted or hashed
4. Use of on blockchain programming (distributed applications, or DApps) to control posting and querying
5. URN and URI formats of identifiers (SGTIN, GLN, SSCC, etc.) are used
6. Use of EPCIS Event and Query data
7. Use of EPCIS EventID to reference events
8. Use of EPCIS standard "ErrorDeclaration" to indicate that an Event identified by the EventID is voided
9. Correcting Events must be posted for events declared in error

Feature observations

Governance:

All sensitive DSCSA data is stored off the blockchain in private repositories controlled by the supply chain stakeholder or their solution provider. Indicators based on industry consensus are stored on the Industry blockchain. It is most likely that the effort of governance will be much lower than ReferenceModel 1, as the states may prove to expose less confidential data and a bit higher than ReferenceModel 2. Consensus on the indicators may only be needed initially or upon addition of indicators.

Operations:

Retrieving actionable data is straightforward. The hash of the SGTIN or SSCC is the distributed application name. Supply chain partners obtain the SGTIN or SSCC of the outer packaging layer from the item's barcode. No evaluation of EPCIS event sets is necessary by individual trading partners. No dependency on individual EPCIS Repository latency.

Risk:

Low: The distributed application is verified and agreed by the industry and regulators. Validation of that code is provided to all. The executed code is visible to all. Low risk to industry stakeholders and regulators.

Cost:

The main governance activities are to form consensus on the rules and logic that would be used to determine the state of the package, as well as the actions to be taken if trading partners should be alerted if the state is incorrect for the incoming event. *For example*, a package with the state of "fit for commerce" is false and the incoming event is a forward logistics shipping event (*the trading partner is trying to ship a package that is not fit for commerce*).

[23] Private, permissioned blockchain platforms allow industries to choose high performing network nodes and set and enforce criteria or rules for companies to access the blockchain.

Compliance:

Letter of DSCSA Law:

ReferenceModel 3 fulfills letter of the law in that it includes addresses for the full DSCSA data set either in individual EPCIS Repositories, or Repositories accessible by blockchain programming.

Intent of DSCSA Law:

Duplicates not possible.

Supply chain integrity:

Counterfeits:

Each legitimately commissioned item will have one (*and only one*) entry. Duplicates are not possible. A manufacturer (or repackager) would be alerted immediately if another distributed application with the same identifier existed.

Theft and reentry:

ReferenceModel 3 allows for "Recall" and other events ("stolen") to be posted and reflected in the indicators (Fit for Use).

Exception management:

EPCIS contains an "ErrorDeclaration" element that can be used to indicate that a EPCIS Event is in error and to identify the replacing event. The programming would reverse the previous indicator settings and apply the new ones.

Note: Reconfiguring the indicators may create an issue for supply chain partners that have already processed the item. Future work in this area should explore whether these supply chain partners receive an alert to the changes and on what states an alert might be given.

SWOT analysis:

Strengths:

1. Provides actionable information to trading partners. Certain trading partners, processing high quantities with very short time limits may not have the luxury of time to evaluate a series of EPCIS events for each and evert package that move through their operation each night.
2. Provides one source of truth that can be trusted by trading partners and regulatory authorities.
3. Reduces the data load and processing time for trading partners.

Weaknesses

1. Obfuscating data and making it accessible and interpretable by the correct parties is an issue with this and all models.
2. Although Provenance is one of the states, there are issues with determining whether a clear set of TIs have been encountered (*trading partners using more than one entity identifier, non-participating trading partners*).
3. If encryption keys are used to protect the data in a repository, key management may be complex and costly.

Opportunities:

1. Could be expanded to provide many kinds of data to serve operational, clinical and contractional processes.
2. Provides one source to connect to other systems (Product Master Data, Temperature Monitoring, etc.).
3. As with ReferenceModel 1, this model can detect duplicate entries, representing legitimate, correctable errors, or potentially counterfeit product.

Threats:

The obfuscation mechanism (*using blockchain oracles*[24] *to interact with encrypt and decrypt data*) may provide a single point of attack.

Observations:

This model attempts to move from duplicating the history of separately evaluating transactions to determine actions to a consensus-based view of items in the supply chain. It could reduce the "re"-processes (*reorders, reshipping, reconciliation, reimbursements, etc.*).

[24] Specialized applications on the blockchain, provided as a service, to retrieve data that is not stored on the blockchain. For example, retrieving ambient temperature for a specific location from a trusted weather service.

ReferenceModel 3:

Life cycle of a pharmaceutical package

Posting data to the blockchain

As an example of the use of ReferenceModel 3 (*where states are determined by industry agreed DApps and minimal data about the product*), package, Lot and shipment are posted to the blockchain provide trading partners actionable information without having to individually evaluate a series of EPCIS events. Prior to transacting, trading partners (manufacturer, wholesaler, dispenser) would exchange their blockchain Account ID and possibly public keys (to decrypt posted transactions). The manufacturer would also post minimal product master data.

A manufacturer would create and hold EPCIS events as product is labeled, packed into cases, packed onto pallets and shipped to the purchasing wholesaler. Upon shipping the product to the wholesaler, the manufacturer would call a DApp, using the held EPCIS event dataset as parameters. The DApp evaluates the data and sets certain states and information for the Lot, package or shipment. The wholesaler would receive an alert that a shipment was posted and could then query the blockchain using the following (*may be masked or hashed*):

Table 2: *Query Parameters*

Query parameter (urn format)	Retrieves
GTIN (Global Trade Item Number)	Limited product master data required by DSCSA + Does product fall under the DSCSA statute.
SSCC (Serial Shipping Container Code)	Hierarchy of the shipment (pallet, cases, packages). Used for receiving.
LGTIN (Lot Global Trade Item Number)	Lot level information: Lot #, Expiration Date, Recall State of the Lot, Is Lot Grandfathered?
SGTIN (Serialized Global Trade Item Number)	Package SGTIN placed in commerce? Fit for Commerce (*no events such as recall, damage or expiration*)? Provenance exists? Declared emergency (may not have DSCSA TI data because it participated in shipments during a declared emergency).

This process would be repeated for the transaction between the wholesaler and dispenser as depicted in **Figure 13**.

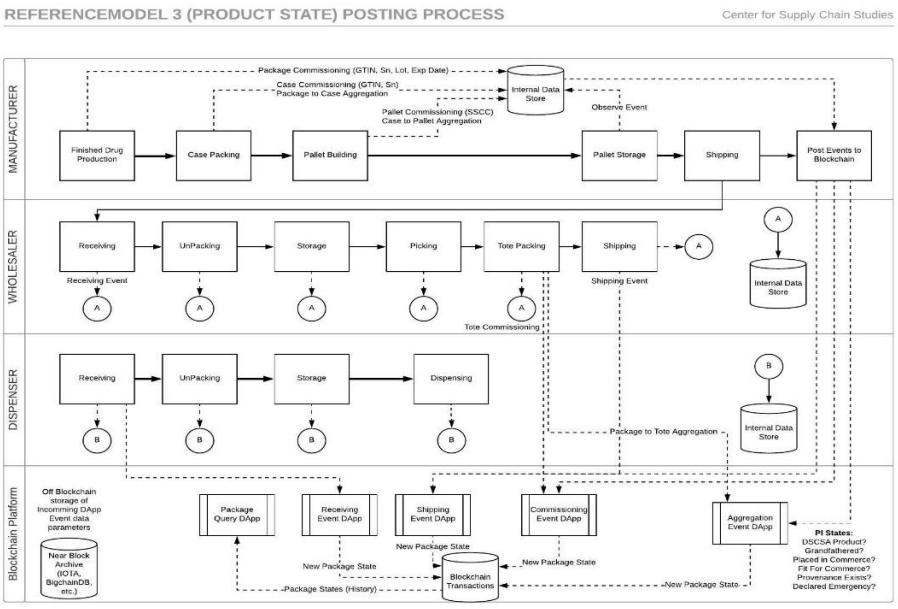

Figure 13:
ReferenceModel 3 – *Posting to the Blockchain*

Verifying that manufacturer placed a package into commerce

As the DApps have evaluated incoming EPCIS transactions according to industry agreement, the trading partner has enough information from the receiving process outlined above to determine whether a package was placed into commerce.

However, if the trading partner would like a second check (*incase additional events have caused the package's state to change*), the trading partner would query the blockchain using the URN format of the GTIN, LGTIN or SGTIN (most likely, the hashed value of the URN format with a unique seed value to keep the data confidential). The retrieved states will provide the trading partner with information that is actionable without evaluation of individual EPCIS events.

Using ReferenceModel 2, the trading partner could query the blockchain to retrieve all states of the package, lot, product or shipment. The states would show whether the manufacturer, or anyone else in the supply chain, had posted an event that would render the product unusable (recall, damage, expired, etc.). **Figure 14** diagrams the verification process for the sample wholesaler and dispenser.

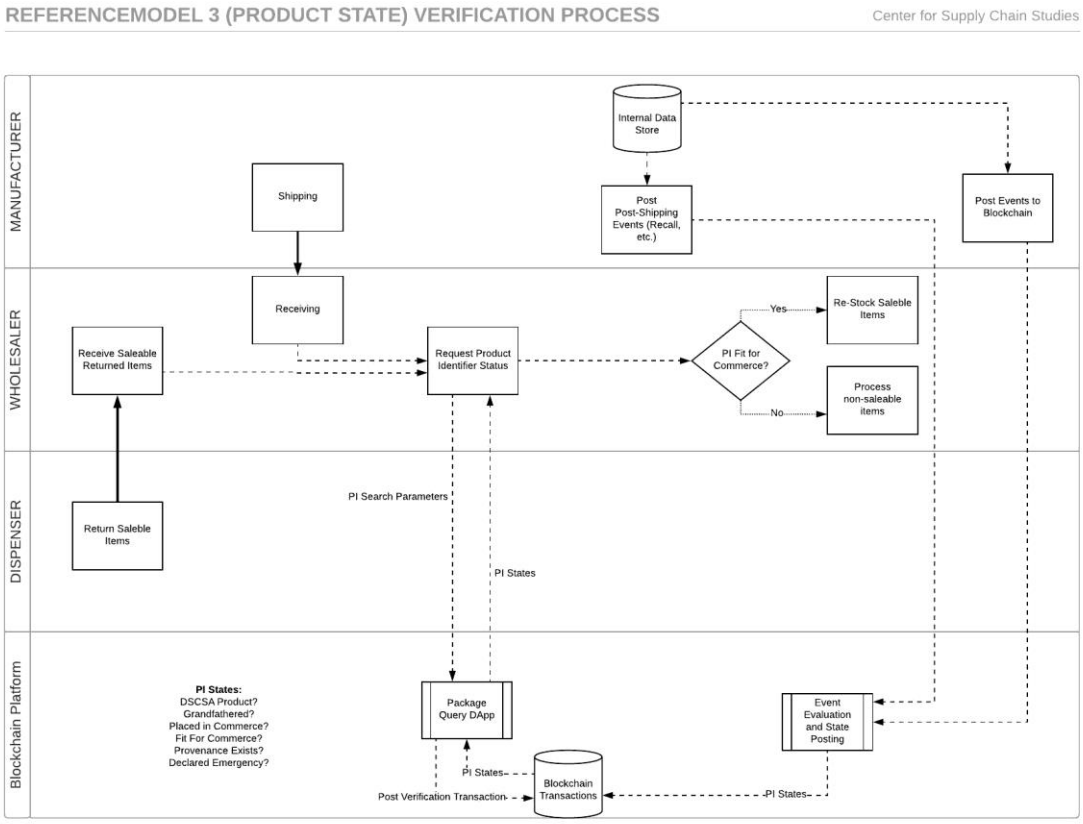

Figure 14:
ReferenceModel 3 – *Verification*

ReferenceModel 3:
The Data

The data depicted in **Figure 15** is non-normative and was used to experiment with placing the TI data on the blockchain. It shows the data that each trading partner holds internally and the data that is posted to the blockchain platform.

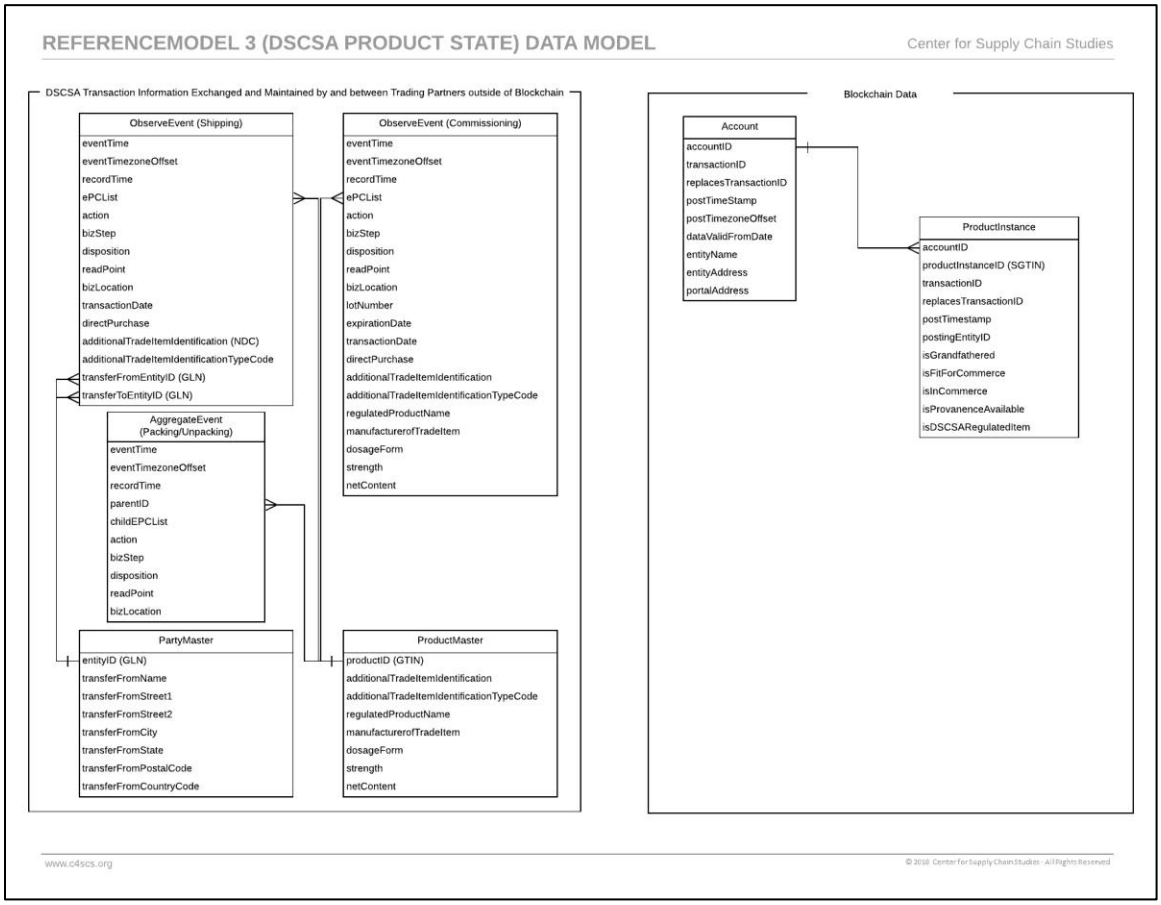

Figure 15:
ReferenceModel 3 – *Trading Partner and Blockchain Data*

ReferenceModel 3+:
The Data

The data depicted in **Figure 16** is non-normative and was used to experiment with placing the TI data on the blockchain. It expands on the "state" concept of ReferenceModel 3 by logically grouping data that may be interesting to query and provides "state" information at the correct group level efficiently.

For example: Determining whether a product is a DSCSA regulated drug is recorded at the product level ("isDSCSARegulatedItem") and not repeated for each package of the product (at the Product Instance level). It shows the data that each trading partner holds internally and the data that is posted to the blockchain platform.

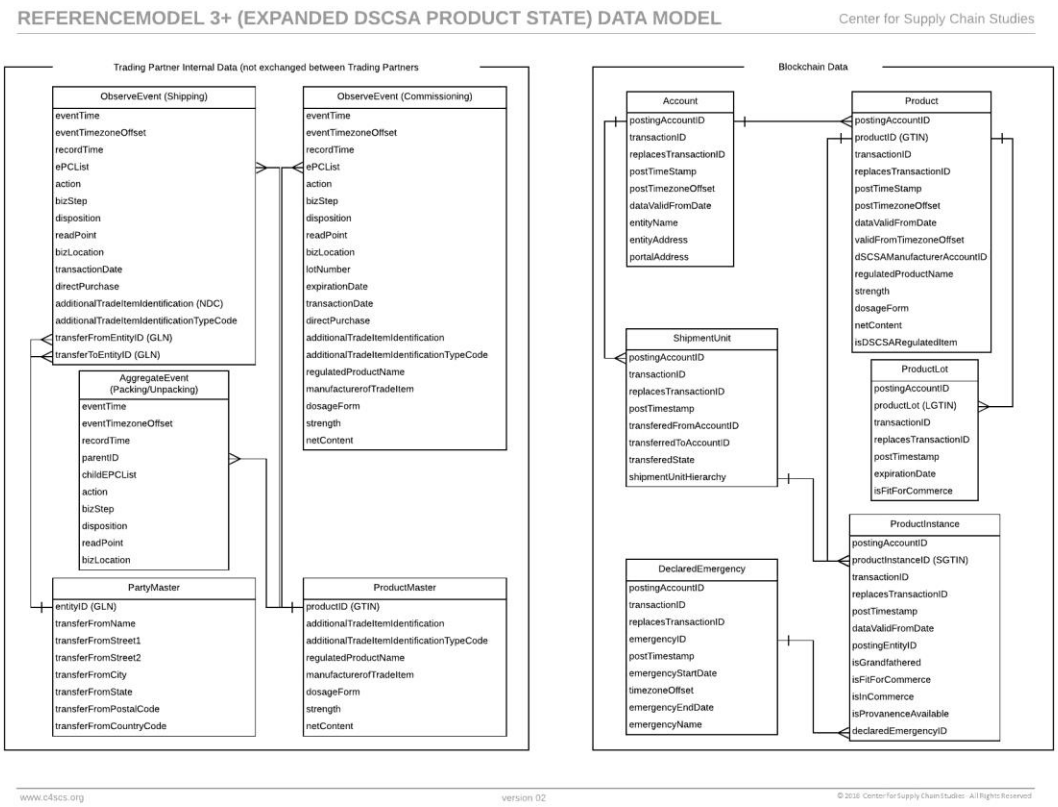

Figure 16:
Expanded data model to support additional value

Evaluating the ReferenceModels

As this was an exploratory Study, we expected to discover and consider different means to utilize blockchain technology to support DSCSA requirements. We hoped this type of examination would provide a platform for learning about supply chain processes, the DSCSA, blockchain technology and the intersection of all three.

All three of this Study's ReferenceModels incorporated different strategies for leveraging blockchain technology – each exposed technical challenges and provided insights into the difficulties of accurately managing product at the serialized package level and at a speed needed by the supply chain.

Not surprisingly, with each strategy we encountered a common set of obstacles that are general to transacting business using a common, visible platform such as blockchain. The challenge of searching for information – while at the same time constraining access to that information to trading partners that have had ownership of the package – is a difficult task (*even with the knowledge that the information may exist*). In all models, this resulted in a multi-step process of evaluating the query and determining whether the querying party should have access to the data.

The following evaluation provides an overview of the Study team's insights into the challenges and benefits of each ReferenceModel. The final take-away from the group is that many of the industry's current regulatory challenges may be successfully addressed as blockchain (and supporting) technology continues to evolve.

With an overarching awareness of the importance of supply chain integrity and protection, we believe it is possible to provide effective, secure and innovative ways of doing business with blockchain technology.

The models and DSCSA requirements

The following requirements are the main data exchange requirements of the DSCSA. The evaluation of the three ReferenceModels reflect the commentary of the Study team participants.

Table 3: *DSCSA Requirements and the Models*

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
Passing TI to next trading partner	Via direct transfer of EPCIS Events	Via direct transfer of EPCIS Events	Via direct transfer of EPCIS Events	Via Shipment Unit blockchain entry
Saleable Returns Verification	Via bizStep of "commissioning" in the posted *ObserveEvent*	1. Retrieve portal addresses from blockchain 2. Via the manufacturer (or repackager) portal or EPCIS repository return of commissioning event	Via *isInCommerce* and *isFitForCommerce* flags in ProductInstance	Via is*InCommerce* and *isFitForCommerce* flags in ProductInstance
Retrieving previous TI back to manufacturer	Via a combination of Observe Events (commissioning and shipping) and Aggregation Events (packing)	Via series of blockchain data queries and query submissions to the portal addresses provided from the blockchain response	Via *isProvananceAvailable* flag (know that an unbroken chain of ownership exists). Retrieve TI data via querying the account's portal address as in ReferenceModel 2.	Via Shipment Unit, Product, ProductInstance data posted to blockchain
Recall	Manufacturer can post Observe Event with bizStep = "inspecting" and disposition = "recalled"	Upon TI retrieval *(see retrieving TI above)*, manufacturer can include an Observe Event with bizStep = "inspecting" and disposition = "recalled"	Manufacturer sends Recall Event data in form of parameters to a DApp which evaluates data and sets *isFitForCommerce* flag in Product Instance blockchain entry	Manufacturer sends Recall Event data in form of parameters to a DApp which evaluates data and sets *isFitForCommerce* flag in Product Lot dataset or Product Instance blockchain entry
Related Requirements				
Proof that data hasn't been altered	All TI data is on the blockchain and is unalterable	Hash value for the TI data is posted on the blockchain and can be matched against the calculated hash value on TI data, retrieved via the trading partner portal address	DApp posts blockchain entries based on consensus rules and data provided as parameters by authoring entity	DApp posts blockchain entries based on consensus rules and data provided as parameters by authoring entity

Measuring the models against stakeholder needs

The following notable needs were identified by the supply chain stakeholders in the Study. The evaluation of the three ReferenceModels reflect the commentary of the Study team participants.

Table 4: *Supply Chain Stakeholder Needs and Models*

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
MANUFACTURER				
Eliminate verification queries	Yes	No	Yes	Yes
WHOLESALER				
Remove need for separate TI events outside of blockchain	No	No	No	Yes
Provide consolidated logistic unit hierarchy	No	No, but possible	No	Yes
DISPENSER				
Reduce verification queries	Yes, 1 query per package	No, 1 portal address query and one TI retrieval Query. Could be able to manage queries for a list of packages.	Yes, 1 query per package	Yes, 1 query per shipment (for 1st wholesaler), 1 query per package for all others.
ALL				
Individual control of authored data access	No, TI data is posted and accessed based on industry set rules	Yes, TI is passed via EPCIS events and all Trading parties query your portal individually	Partial, package state(s) are determined by implemented industry set rules	Partial, package, product and shipment state(s) are determined by implemented industry set rules

The models and Study goals

The following goals were determined at the beginning of the Study. The evaluation of the three ReferenceModels reflects the commentary of the Study team participants.

1. Establishing an electronic connection between non-adjacent trading partners
2. Establishing trust between these trading partners
3. Sharing required data without inadvertently exposing proprietary information
4. Reducing the potential activity required of trading partners
5. Designing for expansion beyond DSCSA compliance
6. Funding the architecture.
7. Reducing risk

Table 5 depicts how the models performed against the initial seven goals of the Study.

Table 5: *Study Goals and the Models*

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
Electronic Connection	Simplified for blockchain, however, still need individual connections between trading partners (RM02 & RM03).			Individual connections not needed.
Trust	Managed through permissioned access to posted data	Managed by each trading partner portal	Managed by Industry consensus on DApps	Managed by Industry consensus on DApps
Confidentiality				
Efficiency	Simple post of event data to blockchain to facilitate TI gathering, however, may require separate send of TI data directly to next trading partner.	Requires separate send of TI data directly to next trading partner. Retrieval of TI data is a 2-step process (1. Retrieve the portal addresses, 2. Query the portals). May benefit from a bulk query (list of serialized items to verify or retrieve).	Up-front work of evaluating the event data is performed by the DApp(s) on the blockchain. Trading partners retrieve and check the latest states(s) for a package instead of a series of events.	Up-front work of evaluating the event data is performed by the DApp(s) on the blockchain. Trading partners retrieve and check the latest states(s) for a package instead of a series of events. Additional efficiency of determining product level and lot level questions with one query.
Expanded value	This model could be expanded by adding new datasets or adding to the existing ones. As the Observe Event dataset contains elements that are not logically grouped, there could be some issues adding new datasets.	This model could be expanded by adding additional datasets and API (s) to trading partner portals. However, making the community aware that a new feature or dataset is available may be difficult.	This model has been expanded to create ReferenceModel 3+.	Can expand to include additional level of information for products (temperature handling instructions), lots (recall), shipments.

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
Funding	Funding models for the shared infrastructure are the same for all ReferenceModels. Membership fees, fees per transactions and utilization of stable cryptocurrencies to fund necessary processing and storage usage. Funding for company-specific repositories will be the responsibility of each trading partner.			
Risk	If trading partners have different interpretations of a series of events a package was involved in. Secondary risk is synchronizing trading partner movement to the same version of event structure. Timing of event posting could cause delays for trading partners processing.	**1**. If trading partner portal is offline, data cannot be verified. **2.** If trading partner accessing portal cannot recall procedures for each repository, performance could be degraded, and labor hours lost.	Risk is mitigated by the industry-agreed DApps that evaluate the events to determine the state(s) of each package. There is risk of missing a state change if the event is not sent to the blockchain DApp(s).	Risk is mitigated by the industry-agreed DApps that evaluate the events to determine the state(s) of each package. There is risk of missing a state change if the event is not sent to the blockchain DApp(s).

Measuring the models against the challenges

The challenges listed in **Table 6** were identified throughout the Study. The evaluation of the three ReferenceModels reflect the commentary of the Study team participants.

Table 6: *Challenges and the Models*

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
		DSCSA		
Multi-link transactions (M-W-D, M-W1-W2-D)	EPCIS events are passed outside of the blockchain. To provide access to event data on an individual package, events are stored at the package level. *eg: individual commissioning events.*	EPCIS events are passed outside of the blockchain.	EPCIS events are passed outside of the blockchain. Stores the "states" of the package as it moves through the supply chain.	Provides shipment hierarchy for each shipment along a package's route. Provides information at the product and Lot level that can be shared with subsequent trading partners.
SEC. 203(g)(1)(E) of the DSCSA – Retrieving previous TI data (2023)	Each trading partner's TI data is stored and can be shared with other trading partners based on industry set rules.	To provide query access to retrieve TI data on an individual package, package level ID is associated with the creating account ID.	Each trading partner's events are provided to a blockchain DApp, which stores the new "state(s)" of the package.	Data is available at many levels (shipment, product, Lot and instance) to respond to queries. DApp(s) post the information and new "state(s)". A portal address is available to query the authoring company directly.
2019, Verification of saleable returns	Commissioning data for each package is available.	Commissioning data for each package is available through the manufacturer's portal.	The *"isInCommerce"* indicator is set for each package.	The *"isInCommerce"* indicator is set for each package.

	ReferenceModel 1 TI/TS Ledger	ReferenceModel 2 Directory	ReferenceModel 3 Package State	ReferenceModel 3+ Expanded States
Supply Chain				
Multiple company identifiers	This challenges all models. It can be solved either by strictly using a single GLN or blockchain Account ID per company or by introducing a company hierarchy look up service.			
Data Access Governance	Must be managed by rules set by industry consensus.	Is managed by individual trading partners in response to TI data queries.	Must be managed by rules set by industry consensus.	Must be managed by rules set by industry consensus.
Blockchain				
Obfuscating data on the Blockchain	This challenges all models. The ability to hide data from a blockchain participant while allowing them to query for data requires special capabilities of a blockchain. The team discussed and experimented with DApp oracles to encrypt data, zero knowledge proofs and other mechanisms. Some blockchain platforms are developing mechanisms to allow querying and obfuscation through special on blockchain processes.			
Data storage limitations	Quite a bit of data is stored in this model. However, private blockchain platforms (vs public blockchains) can manage larger amounts of data.	Minimal data is stored in this model.	Minimal data is stored in this model.	Data is stored across a data model. Each blockchain transaction stores minimal data.
Multiple Platforms	This challenge affects all models. If industry data is spread across multiple blockchain platforms, it is unknown how industry set data access rules would be enforced. There are blockchain/database hybrid solutions (BigchainDB) and other blockchain-like platforms that might be useful. A single platform may be needed in the near term as the technology evolves and solutions are developed.			
Cost	This challenge affects all models. Whether blockchain token or cryptocurrency usage will be acceptable to the industry, traditionally negotiated contract with service providers or some mix of each will emerge to settle the cost/funding model.			

Other Study findings and thoughts

Public and private blockchains

It is generally thought that private, permissioned blockchain platforms are safer than public platforms. That public platform suffers from the following problems:

1. **Performance and storage bloat.** Public blockchains will be subject to a wide range of transactions unrelated to the pharma supply chain. They will create contention for rapid processing of transactions, slowing the processing time. It will also create a much large data storage requirement because storing the entire blockchain would include the millions of non-pharma transactions.
2. **Governance risk.** Over time, blockchain governing groups make changes to their blockchains to address various issues that may arise. In a public blockchain, these changes may not be agreeable to the pharma trading partners, but they may be outvoted. In a private blockchain, the rules and changes will be determined solely by the pharma trading-partner members.
3. **Increased risk of compromise.** Nefarious actors could attack the blockchain whether it is public or private. But, the public blockchain is out in the open for them to study to determine vectors of attack. A private blockchain would be less visible (*so that many nefarious actors might not even be aware of it*) and afford less opportunity for planning an attack.

Protecting the confidentiality of information on blockchains

Most current blockchain platforms make transactions posted to a blockchain visible to all entities that are connected to the blockchain. This visibility is a double-edged sword. It allows anyone to determine if data has been tampered with (by checking the block hash values), but it also allows any connected entity to read posted data and assess the blockchain data for patterns.

All three reference models specify that data posted on the blockchain be obfuscated. However, they don't specify *how*. The team has explored encryption, digital signatures and in one instance, zero knowledge proofs. Additional models not considered here use still other techniques to provide the necessary confidentiality. All have merit, and all have drawbacks in terms of key management, additional services needed, etc. The team also recognizes the challenges of establishing confidentiality in an open platform (even in private/permissioned platforms) and the issues that may be encountered in key archiving and transferal as part of mergers or acquisitions.

Governance

Regardless of the solution selected to address DSCSA (*whether it includes a blockchain component or not*) the requirement of an interoperable solution imposes a significant demand on the industry to establish the governance rules needed for compliance. This calls for developing a consensus among all the stakeholders on dozens of rules of engagement – each of whom may require hundreds of decisions to formulate.

Because the industry is composed of hundreds of trading partners ranging from small to huge, weak to powerful, sophisticated to unsophisticated – providing a wide variety of services along the supply chain path for thousands of products and achieving this consensus will be a difficult and time-consuming effort. Even if all parties were to agree today to implement one of the ReferenceModels™ described above, it will take a long time to establish a consensus on each of these hundreds of decisions that will need to be made.

Next steps

This exploratory Study documented and provided opportunity to explore the supply chain, DSCSA language and blockchain technology. Several challenges were identified, and potential design alternatives thought through. This was the *first step* in readying supply chain stakeholders and solution providers to define the interoperable system needed to satisfy the requirements of the "Enhanced Drug Distribution System" outlined in the DSCSA.

As supply chain stakeholders are currently working through serialization of drug products, there are not enough of them to fully pilot any of the ReferenceModel designs. The next steps are to move from a simulated environment to test environments where the technology can be explored using test or simulated data. This phase will give clarity on implementation issues – testing potential back-end integration and solution-to-solution interoperability. Once the stakeholders begin to converge on single model and can engage in connecting internal systems to a test environment, full pilots and implementations will follow.

Pilots that connect trading partners will provide the information needed to determine standards and guideline development, easing the development of production systems.

Appendix

Terms

DSCSA: Drug Supply Chain Security Act[25]

Tracing Requirement: Effective November 2023, the DSCSA law reads: ``*SEC. 203(g)(1)(E) The systems and processes necessary to promptly facilitate gathering the information necessary to produce the transaction information for each transaction going back to the manufacturer, as applicable, shall be required."*

Obfuscation: For the purposes of this white paper, obfuscation means masking or otherwise making the value of the attributes unknowable to parties other than the creator and those parties. The creator or their proxy give the capability to unmask or otherwise know the value of the attributes.

Trading Partner: Participant in the US drug supply chain. The DSCSA identifies the following trading partner types (see definitions in the DSCSA[26]):

- Manufacturer
- Repackager
- Wholesale Distributor
- Third Party Logistics Provider (3PL)
- Dispenser

Blockchain oracle: A specialized distributed application (DApp) provided as a service to allow blockchain distributed applications to access data outside of the blockchain. *For example, an oracle could provide ambient temperature data from a trusted weather bureau.*

Service Provider: A company that provides data access services to supply chain participating companies.

Transaction Information: Defined in the DSCSA as:

TRANSACTION INFORMATION —The term 'transaction information' means—
"(A) the proprietary or established name or names of the product;
"(B) the strength and dosage form of the product;
"(C) the National Drug Code number of the product;
"(D) the container size;
"(E) the number of containers;
"(F) the lot number of the product;
"(G) the date of the transaction;
"(H) the date of the shipment, if more than 24 hours after the date of the transaction;
"(I) the business name and address of the person from whom ownership is being transferred; and
"(J) the business name and address of the person to whom ownership is being transferred."

Transaction Statement: Defined in the DSCSA as:

TRANSACTION STATEMENT. — The 'transaction statement' is a statement, in paper or electronic form, that the entity transferring ownership in a transaction —
"(A) is authorized as required under the Drug Supply Chain Security Act;
"(B) received the product from a person that is authorized as required under the Drug Supply Chain Security Act;
"(C) received transaction information and a transaction statement from the prior owner of the product, as required under section 582;
"(D) did not knowingly ship a suspect or illegitimate product;
"(E) had systems and processes in place to comply with verification requirements under section 582;
"(F) did not knowingly provide false transaction information; and
"(G) did not knowingly alter the transaction history."

[25] https://www.fda.gov/drugs/drugsafety/drugintegrityandsupplychainsecurity/drugsupplychainsecurityact/default.htm
[26] https://www.gpo.gov/fdsys/pkg/PLAW-113publ54/pdf/PLAW-113publ54.pdf

Use of SWOT analysis

The Study team evaluated the ReferenceModels based on their understanding of the fit of the model DSCSA compliance, supply chain operations blockchain technology and governance. The team also evaluated the ReferenceModels using the initial goals that were set at the beginning of the Study. Lastly, we evaluated based on traditional SWOT (Strengths, Weaknesses, Opportunities and Threats) to give an overall impression of the ReferenceModels.

Definition of SWOT analysis (or SWOT matrix)[27]

SWOT analysis is a strategic planning technique used to help a person or organization identify the *Strengths*, *Weaknesses*, *Opportunities*, and *Threats* related to business competition or project planning.[1] It is intended to specify the objectives of the business venture or project and identify the internal and external factors that are favorable and unfavorable to achieving those objectives. Users of a SWOT analysis often ask and answer questions to generate meaningful information for each category to make the tool useful and identify their competitive advantage.

Strengths and Weakness are frequently internally-related, while Opportunities and Threats commonly focus on environmental placement.

- **Strengths:** Characteristics of the business or project that give it an advantage over others
- **Weaknesses:** Characteristics of the business that place the business or project at a disadvantage relative to others
- **Opportunities:** Elements in the environment that the business or project could exploit to its advantage
- **Threats:** Elements in the environment that could cause trouble for the business or project

ReferenceModel actors

Each ReferenceModel represents a simple supply chain adhering to a specific data sharing strategy to support DSCSA compliance. ReferenceModels were created to explore alternate strategies or methods of making DSCSA supporting data available to each depicted trading partner. They demonstrate enough product movement variation and information sharing to provide insight into how data-sharing strategies and associated rules could work to support DSCSA compliance.

The processes that are exercised by each trading partner do not represent the exhaustive list of processes that take place. Rather, they were created to exercise the data sharing strategies and rules and to provide enough generated data to explore and compare the strategies.

The following actors were used uniformly in the ReferenceModels to aid in comparing the outcome of the strategies.

Manufacturer 1 (identified as M001): The simulated manufacturer creates the pharmaceutical product by Lot, packages it into cases and then packages those cases onto pallets. Pallets are put away in storage and picked to fulfill large wholesaler orders. Following GS1 EPCIS best practices, data sets extracted from Commissioning, Packing and Shipping events are created and processed according to the model's data sharing strategy.

Wholesaler 1 (identified as W001): This simulated wholesaler represents a large, high throughput, national wholesaler that purchases directly form the manufacturer. It receives the shipment at the pallet level (simulated scan of pallet SSCC), breaks down the pallet to individual cases and breaks down each case and puts away the individual trade items. To reflect realities in a high throughput wholesale environment, the cases and trade items are not scanned during unpacking. Trade Items are scanned at the time of order picking and verified against data made available by the design of the ReferenceModel (reflecting the model's data sharing strategy). Trade items are packed into reusable totes and shipped to either the regional wholesaler (W002) or the dispenser (D001 or D002).

[27] Source: https://en.wikipedia.org/wiki/SWOT_analysis

Wholesaler 2 (identified as W002): This represents a simulated regional wholesaler that purchases from a large national wholesaler (W001). It receives shipments of totes from the national wholesaler and scans the tote upon receipt (simulated scan of tote SSCC). It then breaks down the tote to individual trade items and puts away the individual trade items. Trade Items are scanned at the time of order picking and verified against data made available by the design of the ReferenceModel (*reflecting the model's data sharing strategy*). Trade items are packed into reusable totes and shipped to the dispenser (D001 or D002).

Dispenser 1 (identified as D001): This simulated dispenser represents a hospital facility that purchases from a large national wholesaler (W001) or regional wholesaler (W002). It receives shipments of totes from the national or regional wholesaler and scans the tote upon receipt (simulated scan of tote SSCC). It then breaks down the tote to individual trade items and puts away the individual trade items. The individual trade items are scanned at dispense and verified against data made available by the design of the ReferenceModel (*reflecting the model's data sharing strategy*).

Dispenser 2 (identified as D002): This simulated dispenser represents a large retail pharmacy chain that purchases from a large national wholesaler (W001). It receives shipments of totes at its warehouse and self-distributes to the retail store pharmacy. It then scans the tote upon receipt (*simulated scan of tote SSCC*) and then breaks down the tote to individual trade items and puts away the individual trade items. The individual trade items are scanned as the trade items are picked for pharmacy delivery and verified against data made available by the design of the ReferenceModel (*reflecting the model's data sharing strategy*).

Other ReferenceModel Trading Partners: As the team discussed additional processes and trading partner relationships, partial models were created to explore the data sharing strategies and how they might affect or be affected by these other trading partners in the supply chain. The ReferenceModels published here include only the above trading partner actors. Other trading partners explored were:

- **Virtual Manufacturer (identified as VM001):** This actor is the manufacturer of record in DSCSA terms, however, they have outsourced trade item production to a Contract Manufacturer.
- **Contract Manufacturer (identified as CM001):** This actor manufactures the trade item on behalf of the manufacturer. They also provided needed DSCSA data on behalf of the Manufacturer.
- **Third Party Logistics Provider (identified as 3PL001):** This actor transports shipments from the manufacturer to the wholesaler. It takes possession of the shipment, but not ownership.
- **Reverse Distributor (RD001):** This actor receives trade items destined for destruction. Several sub-models depicted reverse distributors receiving product from a wholesaler, notifies the manufacturer and destroys the trade item.
- **Repackagers:** Although the repackaging operation was discussed, no ReferenceModels were built reflecting this unique process of removing drug product from the manufacturer's packaging, combining it with drug product from other trade items and repackaging into new (different count sized) trade items.

Scenarios used to determine quantity and volume of transactions

Supply Chain Scenario #1:
Manufacturer to Wholesaler to Dispenser

Manufacturer 001 manufacturers and sells Product 01 in 60 count bottles in lots of 40,000. They are packed into 20 count cases. Pallets contain 100 cases.

To describe the production of a Lot in EPCIS terms, the Manufacturer would record:

- 1 Commissioning event listing the 40,000 GTIN/Sn of each bottle
- 2,000 Commissioning events (1 for each Case)
- 2,000 Packing events (1 for each Case)
- 20 Commissioning events (1 for each Pallet)
- 20 Packing events (1 for each pallet)

A Wholesaler orders 100 cases (1 Pallet) of product 01. To describe the items in that shipment, the manufacturer would record and send to the Wholesaler:

- 1 Commissioning event listing the 2,000 units, 100 cases and 1 pallet sold
- 100 Packing events (1 for each case)
- 1 Packing event (for the pallet)
- 1 shipping event (for the pallet)

The Wholesaler would record:

- The 103 events sent by the Manufacturer
- 1 Receiving event (for the Pallet)
- 1 Unpacking event (for the pallet)

A Dispenser orders 5 bottles of Product 01 from the Wholesaler. The Wholesaler would record:

- 1 Unpacking event (for the case)
- 1 Commissioning event (for the Tote)
- 1 Packing event (for the Tote and 5 bottles)
- 1 Commissioning event (for the 5 bottles, extracted from the Manufacturer's Commissioning event)
- 1 Shipping event (for the Tote)

The Wholesaler would send the Dispenser:

- 1 Commissioning event (for the Tote)
- 1 Packing event (for the Tote and 5 bottles)
- 1 Commissioning event (for the 5 bottles, extracted from the Manufacturer's Commissioning event)
- 1 Shipping event (for the Tote)

The Dispenser would record:

- The 4 events sent by the Dispenser
- 1 Receiving event (for the Tote)

Supply Chain Scenario #2:
Manufacturer to Wholesaler 1 to Wholesaler 2 to Dispenser

Manufacturer 001 manufacturers and sells Product 01 in 60 count bottles in lots of 40,000. They are packed into 20 count cases. Pallets contain 100 cases.

To describe the production of a Lot in EPCIS terms, the Manufacturer would record:

- 1 Commissioning event listing the 40,000 GTIN/Sn of each bottle
- 2,000 Commissioning events (1 for each Case)
- 2,000 Packing events (1 for each Case)
- 20 Commissioning events (1 for each pallet)
- 20 Packing events (1 for each pallet)

A national Wholesaler orders 100 cases (1 Pallet) of product 01. To describe the items in that shipment, the manufacturer would record and send to the Wholesaler:

- 1 Commissioning event listing the 2,000 units, 100 cases and 1 pallet sold.
- 100 Packing events (1 for each case)
- 1 Packing event (for the pallet)
- 1 shipping event (for the pallet)

The national Wholesaler would record:

- The 103 events sent by the Manufacturer
- 1 Receiving event (for the pallet)
- 1 Unpacking event (for the pallet)

A regional Wholesaler orders 3 cases of product 01 from the national Wholesaler. The national Wholesaler would record:

- 1 Commissioning event derived from the Manufacturer's that only includes the 3 cases sold to the regional wholesaler
- 3 Packing events derived from the Manufacturer's that only includes the cases and the contents of those cases sold to the regional wholesaler
- 1 Shipping event (for the cases)

The regional Wholesaler would record:

- The 5 events sent by the national Wholesaler
- 3 Receiving events (for the Cases)

A Dispenser orders 5 bottles of Product 01 from the regional Wholesaler. The regional Wholesaler would record:

- 1 Unpacking event (for the case)
- 1 Commissioning event (for the Tote)
- 1 Packing event (for the Tote and 5 bottles)
- 1 Commissioning event (for the 5 bottles, extracted from the national Wholesaler's Commissioning event)
- 1 Shipping event (for the Tote)

The regional Wholesaler would send the Dispenser:

- 1 Commissioning event (for the Tote)
- 1 Packing event (for the Tote and 5 bottles)
- 1 Commissioning event (for the 5 bottles, extracted from the national Wholesaler's Commissioning event)
- 1 Shipping event (for the Tote)

The Dispenser would record:

- The 4 events sent by the Dispenser
- 1 Receiving event (for the Tote)