MediLedger DSCSA Pilot Project

Matt Sample, VP Manufacturing Operations
AmerisourceBergen

AmerisourceBergen
1300 Morris Dr.
Chesterbrook, PA 19087
MSample@amerisourcebergen.com
414-374-6504

AmerisourceBergen AMGEN CardinalHealth CENTER for Supply Chain Studies CHRONICLED

Dermira FedEx FFF enterprises Genentech A Member of the Roche Group GILEAD

GS1 US gsk inmar Lilly MAXOR NATIONAL PHARMACY SERVICES COMPANY McKESSON

Pfizer SANOFI VAXSERVE A SANOFI PASTEUR COMPANY Walgreens Walmart

MediLedger

Table of Contents

FDA Pilot Request: Drug Supply Chain Security Act, 2023

At the beginning of 2019, the FDA requested pilot projects that can demonstrate capabilities or address issues expected in the execution of an electronic interoperable system as outlined in the Drug Supply Chain Security Act (DSCSA). Focusing on the enhanced requirements designated to go into effect in 2023 for package-level tracing, the FDA has requested reports from pilot activities in late 2019 / early 2020 that can inform the agency and industry stakeholders as to possible ways forward to enable compliance with the regulation.

The MediLedger Project brought together companies starting in 2017 to explore using blockchain technology to address the interoperability requirements as outlined in DSCSA. That participation grew to ensure we could meet the FDA's pilot request to represent all aspects of participants in the drug supply chain. Our intention is to deliver a review of how a blockchain based solution could address industry wide interoperability, regardless of participant size, function, or business interest. We wanted to ensure that not only compliance with the law could be met by all parties, but also that potential additional FDA regulations for the increased security of prescription medicines could be achieved.

It is the workgroup's belief that, in the absence of a central point of data sharing as other countries have chosen to implement, the US supply chain will suffer as companies struggle with keeping data accurately and completely shared across a wide variety of partners, systems and technical formats. This means that in the event of a significant public health crisis, stakeholders and agents will struggle to locate and quarantine suspect product in a timely manner, continuing to put patients' lives at stake. We believe we have demonstrated that a well-designed, industry-leading, neutral platform (or well managed interconnected platforms) using the advancements of technology like blockchain can avoid these significant risks.

Table of Participants

Company	Type	Contact	Size: number of employees
AmerisourceBergen	Wholesale Distributor, 3PL	Matt Sample MSample@amerisourcebergen.com	21,000
Amgen	Manufacturer	Nikkhil Vinnakota nikkhilv@amgen.com	21,000

Company	Type	Contact	Size: number of employees
Cardinal Health	Wholesale Distributor, 3PL	Dan Vaught dan.vaught01@cardinalhealth.com	50,000
Center for Supply Chain Studies	Consulting	Robert Celeste rceleste@c4scs.org	1
Chronicled	Solution Provider	Eric Garvin eric@chronicled.com	50
Dermira	Manufacturer	Anna Moua anna.moua@dermira.com Andrew Jacobson Andrew.Jacobson@Dermira.com	100
FedEx	3PL	Rogers Stephens rdstephens@fedex.com	425,000
FFF Enterprises	Wholesale Distributor	Jonathan Hahn jhahn@fffenterprises.com	425
Genentech	Manufacturer	Pablo Medina medina.pablo@gene.com	14,000
Gilead	Manufacturer	Blane Stroh Blane.Stroh@gilead.com	11,000
GS1 US	Industry Standards	Peter Sturtevant psturtevant@gs1us.org	160
GSK	Manufacturer	Gregg Gorniak gregg.a.gorniak@gsk.com	100,000
Inmar	3PL	Garry Church garry.church@inmar.com	2,200
Lilly	Manufacturer	Senthil Rajaratnam rajaratnam_senthil_subramanian@lilly.com	34,000
Maxor	Dispenser	Ryan Slack rslack@maxor.com	1,000
McKesson	Wholesale Distributor, 3PL	Matt Langford matt.langford@mckesson.com	80,000
Novartis (Sandoz)	Manufacturer	Dave Mason dave.mason@novartis.com	125,000
Novo Nordisk	Manufacturer	Cathy Barbic cbbi@novonordisk.com	43,000

Company	Type	Contact	Size: number of employees
Pfizer	Manufacturer	Andrew Schmitt andrew.schmitt@pfizer.com	117,000
Sanofi	Manufacturer	Arthi Nagaraj arthi.nagaraj@sanofi.com	110,000
Vaxserve	Distributor	Kevin Carrozza kevin.carrozza@vaxserve.com	150
Walgreens	Dispenser	Melva Chavoya melva.chavoya@walgreens.com David Brown david.g.brown@walgreens.com	350,000
Walmart	Dispenser	Asma Ishak-Mahdi asma.ishakmahdl@walmart.com	2,100,000

Acronyms

- FDA – Food and Drug Administration
- DSCSA – Drug Supply Chain Security Act
- zk-SNARKs - Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, a mathematical proof concept where possession of information can be proven without revealing that information
- TI – Transaction information
- HIN – Health Industry Number, administered by the Health Industry Business Communications Council
- DEA – Drug Enforcement Agency
- HDA – Healthcare Distribution Alliance
- CCoO – Confidential Change of Ownership
- API – Application Program Interface, a set of routines, protocols, and tools for building software applications
- GTIN – Global Trade Item Number, a family of GS1 global identification data structures

Pilot Description and Report Overview

The MediLedger Pilot was an exploration of the feasibility of using blockchain technology to create an electronic interoperable system as required by the Drug Supply Chain Security Act (DSCSA) in 2023. Chronicled, a technology company, led the discussions and analysis. The participants represent a broad group of industry stakeholders:

- brand manufacturers
- generic manufacturers
- virtual manufacturers
- wholesale distributors
- regional distributors
- pharmacy chains
- reverse logistics
- 3PL / transportation companies
- industry standards bodies

Chronicled's commitment to the industry is to identify how blockchain technology can best serve the overall industry by providing technical and industry expertise along with an objective viewpoint. Their role was to educate companies on how a blockchain based solution could work, and then document the industry's feedback, describing alignment or differences of opinion. The intention of this pilot is to capture the pharma industry's perspective and potential for a blockchain-based interoperable system for enhanced unit level tracking.

At each step of the pilot we were mindful of anti-trust issues to ensure an open and safe dialogue could take place.

This report is broken down into four parts:

- An executive summary to outline the conclusions established in this pilot work
- The approach taken by the group to establish the solution
- A review of the technical approach, along with discussions of specific operational risks
- A vision for use of blockchain

Executive summary

The **MediLedger FDA Pilot Project** brought together some of the world's leading pharmaceutical manufacturers, wholesale distributors, pharmaceutical dispensers, logistics companies, professional organizations, and standards bodies to explore the potential of blockchain technology in the track and trace of prescription medicines. Our scope was to evaluate the feasibility of a blockchain based solution for compliance with The Drug Supply Chain Security Act (DSCSA) requirements related to the interoperable, electronic tracing of products at the saleable unit and homogenous case packaging level.

Based on business requirements and guidance from our project team, we developed a blockchain-based system for tracking the legal change of ownership for prescription medicines in the United States. In summary, the project team has drawn the following conclusions:

- Through this project, we have shown that blockchain has the capability to be the technology underlying an interoperable system for the pharmaceutical supply chain, as mandated by DSCSA, while leveraging GS1 Standard Electronic Product Code Information Services (EPCIS) messaging standards. When using a single blockchain solution, transaction throughput, speed, and reasonable cost can be achieved to meet stakeholder needs.

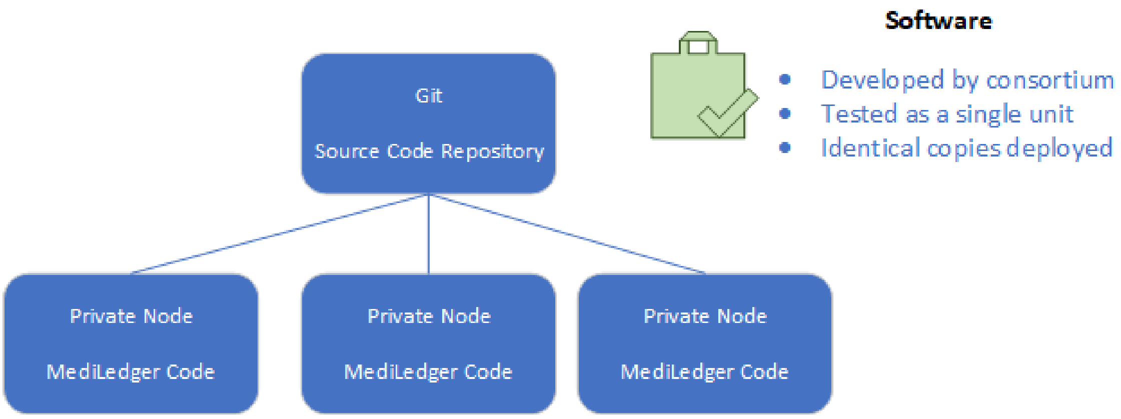
- Data privacy requirements of the pharma industry (Manufacturers, Wholesale Distributors, Dispensers, and 3PLs) can be solved for by using "*zero knowledge proof*" technology, where all transactions posted to the blockchain are fully obfuscated, ensuring no confidential information or business intelligence is shared. The design allows for nodes in the blockchain system to be hosted by multiple unique parties while maintaining strict transactional privacy and still ensuring immutability of the transactions.
- A blockchain system can be capable of validating the authenticity of product identifiers (verification) as well as facilitating the provenance of saleable units back to the originating manufacturer.
- The authenticity of the drug transaction information can be confirmed with each transaction allowing for expedited suspect investigations and recalls.
- The group believes that should a blockchain ecosystem be created as a possible solution to the DSCSA interoperable solution requirement, it should have an open system architecture with an appropriate governance to oversee the function of the system and ensure compliance with industry agreed business rules and standards of operation.
- Governance should come from the industry itself
- The trust established by a blockchain system can be leveraged for a myriad of additional business applications to the pharmaceutical industry, allowing for compounding benefit for this industry once such a platform is established.
- As we see from every step of implementation of DSCSA, this is a complex solution that will require a stabilization period. The implementation date and the FDA enforcement date could be separate and planned in advance.
- The long-term success of a truly interoperable blockchain-based solution will require strong participation and adoption from all industry stakeholders (manufacturers, wholesalers, dispensers, service providers, etc.).
- There are clear challenges with making disparate track and trace systems interoperable. The project group is concerned that no standards currently exist to make the multiple systems interoperable, and without appropriate standards, it is not likely that disparate systems can be made successfully interoperable.

Working Group Approach

The original MediLedger Project working group was established in 2017 to bring together representatives from leading pharmaceutical manufacturers, wholesale distributors, supply chain management experts and various companies to develop business requirements for an interoperable system to meet the 2023 DSCSA requirements. A technical, working prototype that met the industry requirements and the DSCSA requirements was created. In the current FDA Pilot Project, we have added to that work to identify additional components of the future solution. The accomplishments of both efforts are:

- Modeled events in a serialization data exchange environment for prescription drugs using a blockchain-distributed ledger system
- Developed and proposed a business and financial model that allows for the participation of the different industry stakeholders
- Identified potential issues with system performance and capabilities
- Defined the potential IT architecture of an electronic interoperable system
- Shared blockchain knowledge, separating reality from hype
- Demonstrated how blockchain technology may be better suited than other solutions to meet DSCSA requirements while providing other strategic advantages
- Identified industry standards in use for the solution, and standards that would benefit the industry
- Outlined how the system could facilitate solving system and process errors and identify nefarious behavior
- Defined human factors that could present implementation challenges
- Identified a process for onboarding and managing authorized trading partners
- Described possible governance of the system
- Showed how the MediLedger solution could be interoperable with standards like EPCIS
- Created a value proposition for the MediLedger solution

The working group considers that consortium-based software development has proven to be more cost efficient, have higher quality, and show a quicker time to value than traditional unilateral development efforts. Within the consortium, all members share in the development effort to include costs, requirements and testing. The output is a single code base that can be deployed by each company with a high degree of interoperable certainty. This is accomplished by using docker and Kubernetes technologies to build software containers. These software containers can be run by individual companies regardless of their infrastructure implementation.



Software

- Developed by consortium
- Tested as a single unit
- Identical copies deployed

Guiding Principles

The current market of companies offering blockchain based solutions holds a wide variety of approaches. We feel strongly that key principles need to be followed to meet the "ethos" of blockchain and the value that sets blockchain apart from current centralized solutions. This goes beyond simply decentralized operation. Here are the key operating principles:

1. **Industry-First** – The Members aim to address industry problems and needs that require collaboration. New protocols and functionalities are prioritized based on the benefits delivered to the trading partners.
2. **Increase Safety**- The solution should meet or exceed DSCSA requirements and advance patient safety and facilitate the gathering of critical information in the event of a dangerous product.
3. **Inclusive** - The Network is designed to ensure all qualified healthcare industry companies can participate, with no barriers based on size or subjective criteria.
4. **Fair** - All Members have equal opportunities to develop their businesses because the Network facilitates connectivity across all Members. Ensure that costs and benefits are achievable and balanced.
5. **Company Controlled Data** - By leveraging the blockchain and confidential data exchange, the Network is designed to ensure that each Participant's Private Data is owned by such Participant, and each Participant has full control of who and how it shares its Private Data with business partners or for profit. There are misperceptions that Blockchain means full transparency, and that all data needs to be shared with all parties. This is fundamentally not true, and we feel important to clarify: blockchain can enable validation of transactions without requiring data to be shared.
6. **Location and Status Visibility** - One of the keys features of the solution is the ability of the system to know the location and status of a uniquely identified product at any time.
7. **The Point of Dispense as Last Line of Defense** – Countries following the EU Falsified Medical Directive are focused on the importance of capturing the dispense event to "retire" the serial number and allow the point of dispense to be fully informed of any issues on the status of a product such as stolen, recalled or a non-valid serial number. However, this is not part of the DSCSA requirements and therefore the US will not benefit from this level of visibility. As the Pew Charitable Trust mentioned in their 2013 testimony to US Congress on the key elements of a national system, cases of invalid or duplicated serial numbers have happened in the US and could be avoided if the serial number is retired after the drugs were dispensed from the pharmacy. The workgroup participants recognize that DSCSA does not require such scanning and feel it is critical that dispensers and the FDA join efforts like MediLedger to help determine how to resolve this remaining challenge.

Technology Solution

The overall vision of our work was to create a system that could confidentially track the change of ownership of prescription medicines without requiring trading partners to reveal data to each other or require a centralized system to hold the information. Our belief is that a neutral industry platform, which does not exist today, would enable the facilitation of information exchange and proactive validation of rules that would highlight immediately if there were reasons to believe the product was suspect. We believe there is a significant need for such a platform in the US and it would bring the critical benefits that other countries are experiencing with government or consortium run systems without the drawbacks of such approaches.

This section outlines the technical approach taken to achieve this result, standards that already exist and potential gaps in standards, and discussion of some of the concerns around the realities of how the supply chain would operate that could add complexity to such a rigorous rule enforcement system. We believe that such a solution allows the industry as a whole to drive the design so that any misalignment can be identified quickly and solved in a collaborative way that is focused on drug safety.

High Level System Requirements

- Enable every authorized organization in the Pharma industry to plug into the system
- Ensure 100% privacy of data committed to blockchain ledger with zero leakage of business intelligence
- Process 2000+ transactions/second (as determined by industry peak shipment windows)
- Complete verification requests in less than 1 second
- Create specifications to solve aggregation/deaggregation, saleable returns, and exception handling
- Create a level playing field to eliminate potential for vendor lock-in

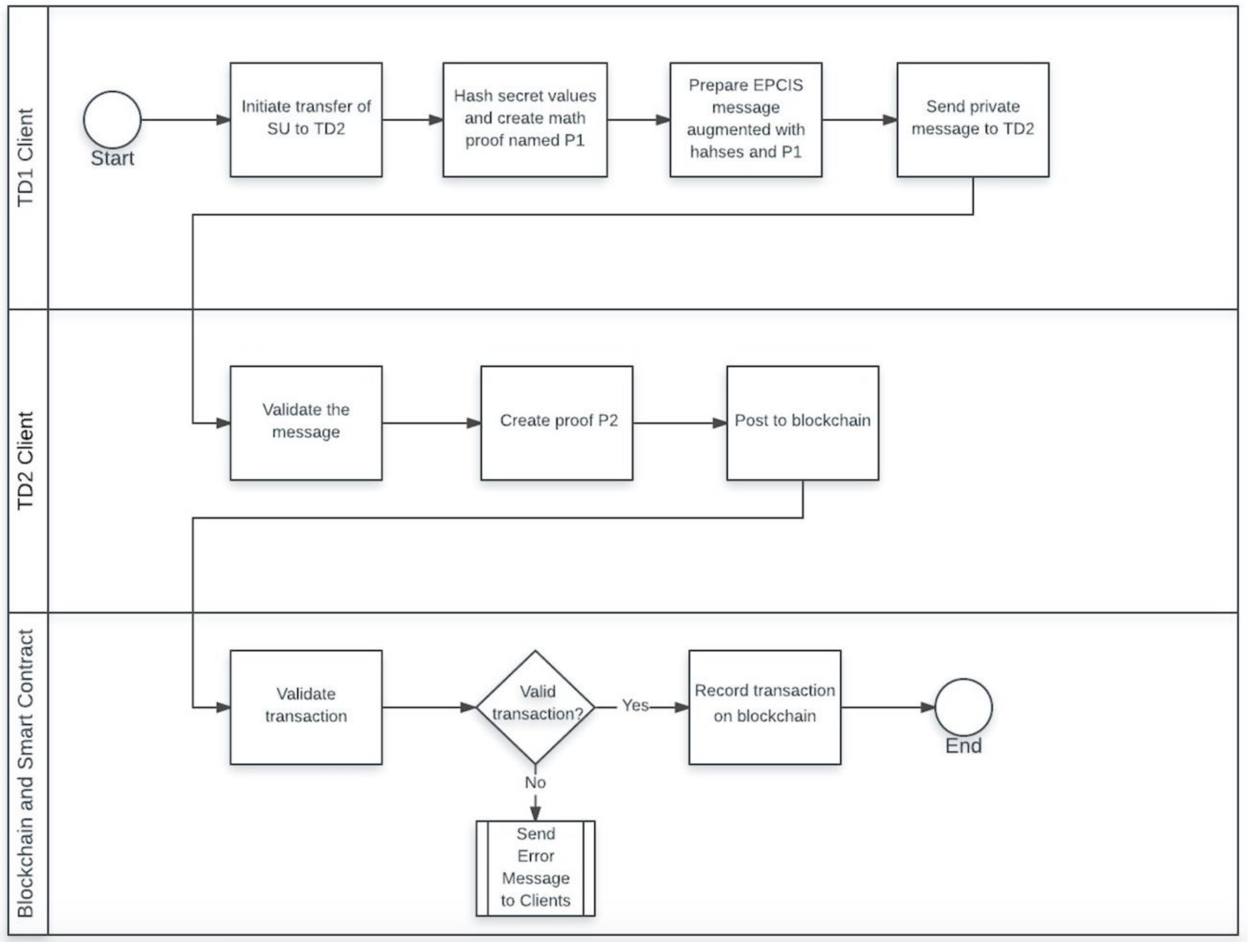
Solution Overview

The solution uses three core technologies:

1. Private messaging between Clients to exchange confidential messages between Trading Partners by leveraging EPCIS standards.
2. Blockchain as a shared, immutable ledger to register the proof of the authenticity of transactions and execute smart contracts. The blockchain will enforce business rules, such as only one company can have legal ownership of a serialized unit at a given time (no double transfer).
3. zk-SNARKs to further enhance privacy by ensuring no business data is revealed.

The key design pattern of the solution focuses on the handling of a serialized unit. Each unit is managed as a non-fungible token with the custody assigned to a trading partner. Custody of a serialized unit can be transferred, and the transfer function is governed by the smart contract deployed on the blockchain. Smart contracts can be designed to enforce business rules which are agreed upon across the industry or across trading partners. The current custodian initiates the transfer and the recipient of the transfer needs to accept it in order to complete the transaction.

The system will ensure that only the authorized manufacturers of a particular product can provision their own serialized units on the blockchain. Then a transfer of a serialized unit (SU) between a trading partner (TD1) and second trading partner (TD2) is described in this diagram (logic is included below):


TD1 Client
Start
Initiate transfer of SU to TD2
Hash secret values and create math proof named P1
Prepare EPCIS message augmented with hahses and P1
Send private message to TD2
TD2 Client
Validate the message
Create proof P2
Post to blockchain
Blockchain and Smart Contract
Validate transaction
Valid transaction?
Yes
No
Record transaction on blockchain
End
Send Error Message to Clients

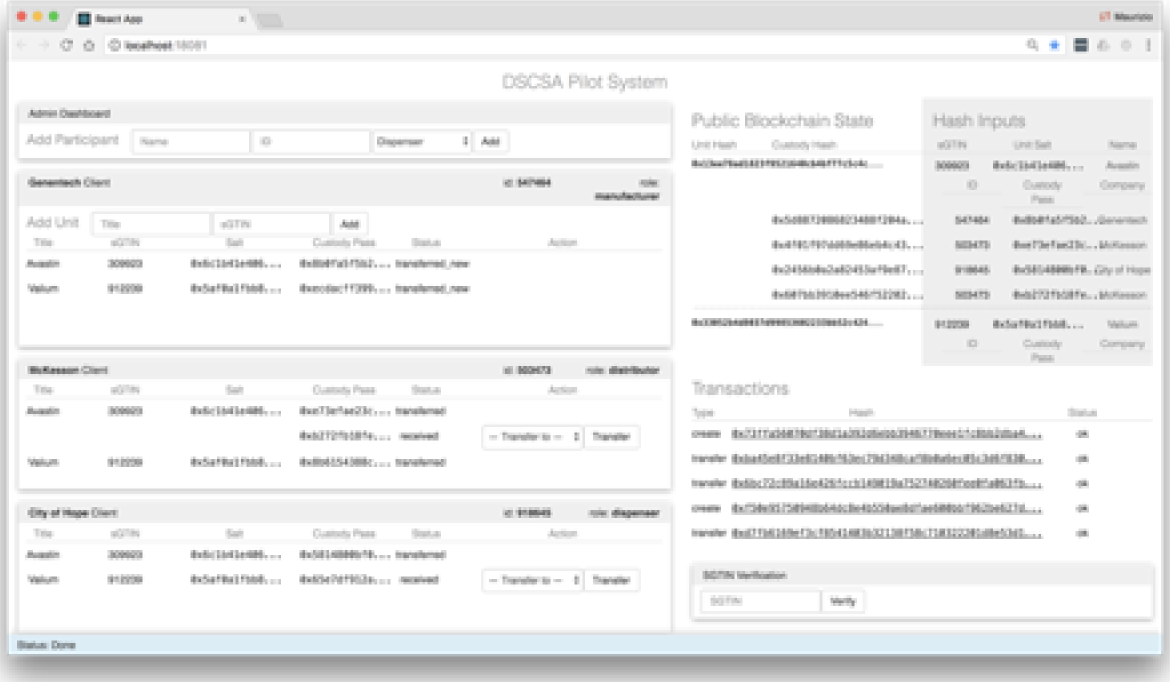
- TD1 Client is instructed via an API call to initiate the transfer of SU to TD2.
- TD1 Client calculates its side of the blockchain transaction, which contains hashes of its secret values and a TD1 mathematical proof named P1.
- TD1 Client prepares an EPCIS message with proper instructions about the transfer (i.e., shipment in a GS1 BizStep).
- TD1 sends a private message to TD2 containing EPCIS data and the TD1 side of the blockchain transaction.
- TD2 formally validates TD1 message and prepares its side of the blockchain message that contains hashes of its secret values and TD2 mathematical proof named P2.

- TD2 posts the transaction to the blockchain.
- The smart contract validates the transaction by verifying both proofs P1 and P2. If valid, the smart contract updates its state by incorporating the hashes submitted in the transaction as part of the new state. These new hash values represent the transfer of custody of SU from TD1 to TD2.
- When utilized in a serialized pharmaceutical supply chain, this process could, for example, move the ownership of a serial number from a distributor to a dispenser in a validated and controlled way. This process ultimately allows a recipient to ensure the matching serialized barcode they are accepting has a fully confirmed chain of custody.

Multiple variants of the solution were implemented and tested in order to confirm specific properties of the system.

Test User Interface

A test user interface was created in the MediLedger Change of Ownership (CCO) prototype for purposes of illustrating the transactions and showing which information is stored on the blockchain. This user interface (UI) would not be part of the completed MediLedger CCO system.



Genentech Client

Title	sGTIN	Salt	Custody Pass	Status	Action
Avastin	309923	0x6c1b41e486...	0x8b0fa5f5b2...	transferred_new	
Valium	912209	0x5af8a1fbb8...	0xecdacff399...	transferred_new	

McKesson Client

Title	sGTIN	Salt	Custody Pass	Status	Action
Avastin	309923	0x6c1b41e486...	0xe73efae23c...	transferred	
			0xb2727b18fe...	received	— Transfer to — Transfer
Valium	912209	0x5af8a1fbb8...	0x8b6154388c...	transferred	

City of Hope Client

Title	sGTIN	Salt	Custody Pass	Status	Action
Avastin	309923	0x6c1b41e486...	0x58148880f8...	transferred	
Valium	912209	0x5af8a1fbb8...	0x65e7df952e...	received	— Transfer to — Transfer

Public Blockchain State / Hash Inputs

Unit Hash	Custody Hash	sGTIN / ID	Unit Salt / Custody Pass	Name / Company
[illegible]		309923	0x6c1b41e486...	Avastin
	0x5d88720868234887284a...	547484	0x8b0fa5f5b2...	Genentech
	0x4f82f97dd69e86eb4c43...	503473	0xe73efae23c...	McKesson
	0x24560d2e82453af9e87...	918645	0x58148880f8...	City of Hope
	0x68f5b3916ee546f52282...	503473	0xb2727b18fe...	McKesson
[illegible]		912209	0x5af8a1fbb8...	Valium

Transactions

Type	Hash	Status
create	[illegible]	ok
transfer	[illegible]	ok
transfer	[illegible]	ok
create	[illegible]	ok
transfer	[illegible]	ok

System Performance

The system performance of the MediLedger CCO protocol was designed to meet business requirements for transaction throughput, which considered the number of prescription medicines in the US (4.5B/year) and an estimate of the number of transactions per unit sold (estimate = 6). This resulted in this calculation for the average number of supply chain transactions per second:

(4,500,000,000 x 6) / (365/24/60/60) = 856.16 transactions/second
# of transactions / number of seconds in a year

The business requirement was 2000 transaction/second.

The results of performance system design are cost-effective performance improvement and accelerated business results. And the key factors for system performance for MediLedger are

- Proof generation on the client
- CPU bound and memory bound factors
- New Jubjub elliptic curve increases performances 5x
- Industry hosted

The steps for proof verification which contribute to performance are:

- Storing transactions and state
- Spring proofs and hashes

The storage bound parameters

- 74 MM transactions/day
- 2,000 transactions/second

These node storage metrics were defined based on the transaction estimates:

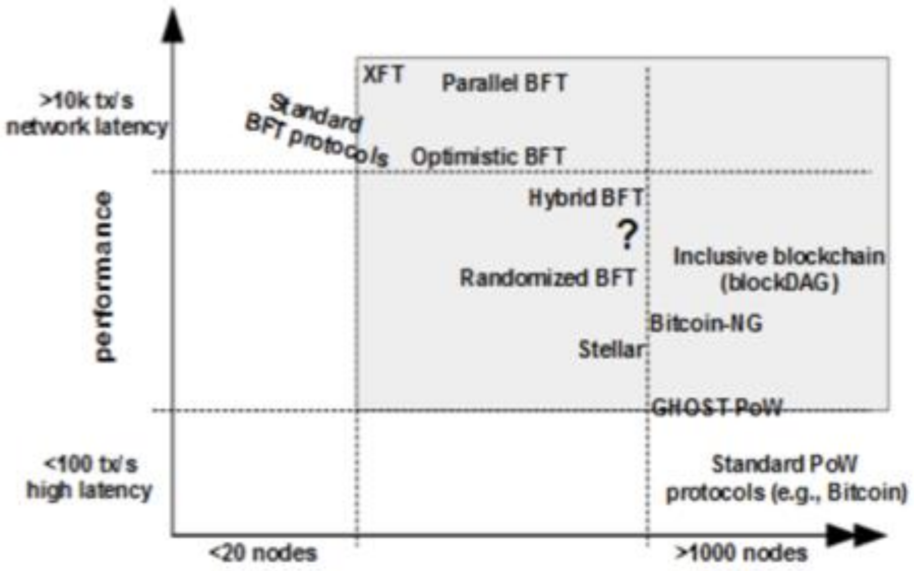
- Number of Tx: 66.5B
- Theoretical storage (based on Ethereum protocol specs):
    - 7 years without transaction pruning: 100TB
    - 7 years with transaction pruning (excluding last year) 26TB
- Actual storage (tested on Parity):
    - 7 years without transaction pruning: 399TB
    - 7 years with transaction pruning (excluding last year): 111.8TB
- Costs of consumer-grade storage purchase
    - 100TB: $4,000
    - 400TB: $16,000
- Node cost for entire Pharma Industry: $5-10M/year

And the client performance was estimated using two different AWS server configurations:

AWS Server	Proofs/Sec	Hashes/Sec	Instances v.1	Instances v.2	Instances v.2 with Jubjub

x1.32xlarge	2,000	V1: 4,600 V2: 46,000	45	445	89
c3.8xlarge	2,000	V1: 4,600 V2: 46,000	158	1,580	316

V.1 – Presented in the demo, based on a hashmap (SGTIN hash -> Custody Hashes)
V.2 – Based on a Merkle tree with absolutely no linkage amongst transactions



The performance conclusion was that cost of storage and client computing was reasonable for a MediLedger track and trace system which would support all of the drug movements of prescription medicines in the US and store this data for seven (7) years.

The MediLedger system could be engineered to meet the business requirement for 2000 transaction/second and would be adequately fast to perform these transactions in near real-time.

Standards

There are a number of standards that the industry has developed that will play a key role in developing interoperable systems to meet the 2023 DSCSA requirements. The intention is to design a solution that relies on existing standards where available rather than create new standards. GS1 has developed standards for Identifying Products (GTIN), Locations (GLN), and Logistic Units (SSCC) Capturing 2D barcodes (GS1 DataMatrix), linear barcodes (GS1-128) and Sharing data with EPCIS. The lightweight Messaging Standard was developed to support DSCSA Verification of Returned

Product Identifiers. This was developed at the recommendation of the HDA Verification Taskforce and solution provider driven work groups.

We are encouraged by the efforts the PDSA workgroups have launched to develop such a governance model, but significant work remains, and we believe that all sectors of the supply chain, federal and state officials will need to be engaged and participate.

Existing industry, GS1 US, and Solution Provider Work

1. Business requirements document
    - Business requirements for requesting, responding and enabling processes for VRS
2. Solutions architecture reference document
    - A framework for defining the recommended VRS components and the necessary system architecture to support saleable returns
3. Lookup directory
    - Requirements for connectivity information upload to the LD and LD synchronization using blockchain.
    - Requirements for connectivity information upload to the LD and LD synchronization using non-blockchain.
    - Translation software to sync a blockchain LD to non-blockchain LD.
4. Request-Response messaging standard
    - The format and content for the Request and Response messages
5. VRS governance body charter
    - Requirements for governance and stewardship including the group's intended objectives, proposed responsibilities, planned activities, expected deliverables, and overall operational parameters and logistics.

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

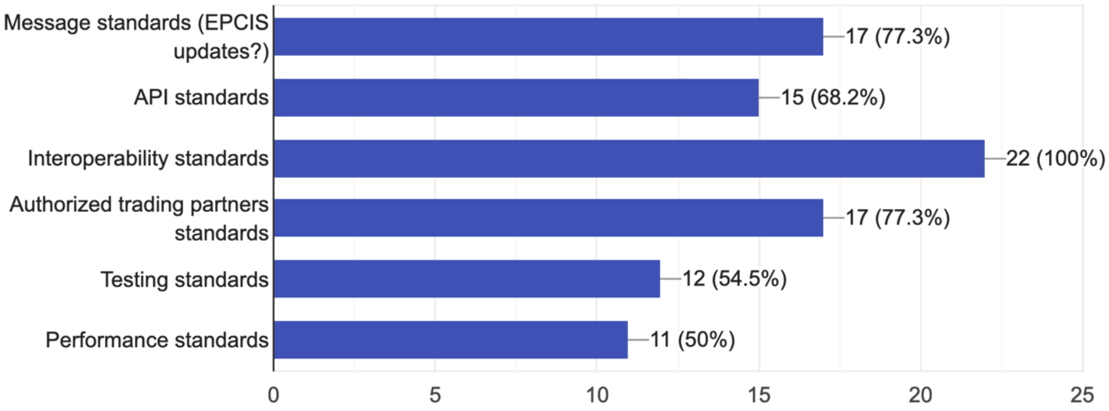
1. GS1 Lightweight Messaging Standard for Verification of Product Identifiers
    - Standardized lightweight messaging framework for asking such verification questions and receiving actionable information that immediately enables the requesting party to determine whether to accept, reject or quarantine a product instance
2. Global Traceability Standard for Healthcare
    - GS1 numbering, Automatic Identification Data Capture (AIDC) and data communication standards that must be in place for traceability
3. Electronic Product Code Information Services (EPCIS)
    - Standards to define EPCIS which enable disparate applications to create and share visibility event data, both within and across enterprises
4. Healthcare GTIN Allocation Rules
    - Consistency in the use of data structures worldwide and specific Point-of-Sale

requirements for Prescription & Non-Prescription healthcare items

5. Healthcare GLN Implementation Guideline
    - Implementation guidance for the use of the GS1 Global Location Number (GLN) in healthcare

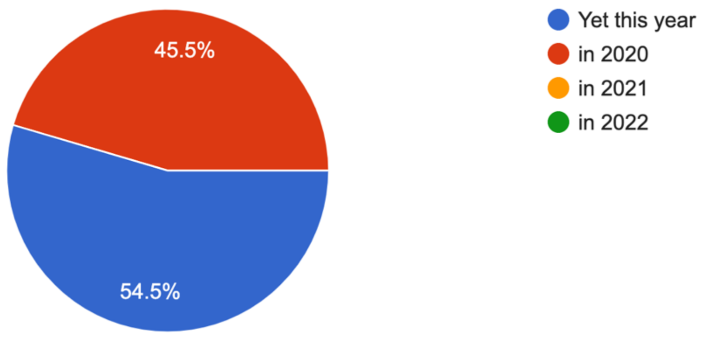
In our discussions in August 2019, pilot participants also identified standards that will be needed for the 2023 implementation of a confidential change of ownership system. Nearly everyone agreed that the four main standards that need to be developed are:

- GS1 Guidance on how to use EPCIS to update product identifier status with downstream trading partners.
- Assuming multiple blockchains and non-blockchain networks may exist, datagram standards on what is being stored and standards on business rules to store that data.
- Processes to ensure authorized trading partner identification.
- Standards and Protocols for recall and alert notification



Many participants in the MediLedger pilot also thought that testing and performance standards would be important to develop, and others also stated that exception handling and status standards should be developed. Nearly all pilot project members believe that GS1 should be the recognized international standards body driving these standards. GS1 will be critical to developing these standards, in addition to other groups that may be outside the industry like BiTA (Blockchain in Transportation Alliance) who are working on technical standards.

We are fast approaching the time that this standard development should begin with half the group stating that it should start immediately, and the other group stating that development needs to start in 2020. Participants highlighted that a relatively simple part of interoperability took the workgroups three years to reach a point of use and we expect the 2023 requirements will be significantly more complex.



Exception Handling

Blockchain technology as the basis for a neutral industry governed platform has a distinct advantage in its ability to make exception handling significantly clearer and easier to manage. In a point to point system network, systems can become quickly misaligned and cause disruption of product flow or dangerous product to go unnoticed. As product moves along the supply chain and ownership changes from upstream partner to downstream partner, there are four main exceptions that could happen in a confidential change of ownership system. In developing these exception handling scenarios, we assumed that we would have full or nearly full participation in one or more interoperable systems. In addition, the following guidelines were used:

- The objective is to reduce interruptions to the flow of medicines (receiving, shipping)
- The business rules and conclusions do not have to be unanimous. The system could be configurable based on participant agreements and governance.
- Product verification can be a tool to manage exceptions and allow transactions to continue.
- The exceptions can manifest themselves at multiple steps in the supply chain but for simplicity we will simulate exceptions at the distributors.

The project group had a vital discussion about how the TI (transaction information) will be updated if the blockchain data is immutable. While it is true that the data on the blockchain cannot be changed or “corrected”, another transfer could be initiated with the data correction which would create a new transaction that corrects the original transaction. In addition, there was a lot of discussion on whether a product verification could be done to correct the TI information, but it was unclear whether or not this would be acceptable to the FDA. This approach is similar to the way that many official records systems work such as car or home titles where corrections to records are made with original incorrect entries left for historic visibility.

In order to avoid a cumbersome corrections process that could delay product and add unneeded cost to the overall supply chain, general principles are needed to enable efficient correction of problems. This is one significant area that the group felt the FDA could add clarity to by providing guidelines for flexibility in correcting system records with sufficient checks and reliability.

These are the exceptions that were identified. Note that in all scenarios, a product verification can be done to confirm the correct production information, and if that verification fails, the product should be treated as suspect. There are additional suspect product scenarios in the next section.

No.	Exception	Description	MediLedger
1	Missing File @ Receipt	Product received @ DC, but EPCIS file was not received for the shipment.	Product No Data during Receipt File Missing
2	Product Overage @ Receipt	Product received @ DC, EPCIS file received, but serial number scanned not in EPCIS file.	Product, No Data during Receipt Overage
3	Product, no Data @ Pick	Product picked, but no serial number found in distributor’s system	Product No Data during Shipping Txn
4	Data, no Product @ Receipt	Received more data than products received.	Data, No Product during Receipt

Each scenario was reviewed with the above guidelines in mind, and the group was able to decide what actions the system should take to facilitate a solution. Each scenario below includes the conditions under which the exception may occur, and systemic solution.

No.	Exception	Description	MediLedger
1	**Missing File @ Receipt**	**Product received @ DC, but EPCIS file was not received for the shipment.**	**Product No Data during Receipt** **File Missing**

Conditions	Systematic Solutions
EPCIS transaction failure Incorrect EPCIS file sent by seller	1. Send a peer to peer message to the seller and request the EPCIS file 2. Send a verification request to the Mfr and upon response: a. VERIFIED: treat the product like a saleable return b. VERIFIED: automatically create a MediLedger transfer transaction c. NOT VERIFIED: indicate the product is suspect

In this scenario, the group noted that the TI may need to be completely resolved by the seller rather than doing verification. The current process of addressing a missing or incorrect ASN file is treated with urgency and the record is corrected before processing continues. The sending and receipt of a peer to peer message would need to be time bound, and an escalation process would need to be created to ensure the issue is resolved quickly.

No.	Exception	Description	MediLedger
2	**Product Overage @ Receipt**	**Product received @ DC, EPCIS file received, but serial number scanned not in EPCIS file.**	**Product, No Data during Receipt Overage**

Conditions	Systematic Solutions
Seller sent more product than was ordered EPCIS file was missing product that was ordered	1. Send a peer to peer message to the seller and request the EPCIS file 2. Send a verification request to the Manufacturer for the extra product and upon response: a. VERIFIED: treat the product like a saleable return b. VERIFIED: automatically create a MediLedger transfer transaction c. NOT VERIFIED: indicate the product is suspect

In Exception Scenario 2, it was noted that the manufacturer would need to know which SN was received that was not in the EPCIS file. In addition, the group was split on whether or not a verification request should be sent in order to receive the product. While 73% of the group did believe the verification request should be sent, 36% of the group did not.

No.	Exception	Description	MediLedger
3	**Product, no Data @ Pick**	**Product picked, but no serial number found in distributor's system**	**Product No Data during Shipping Txn**

Conditions	Systematic Solutions
Aggregation errors	1. Send a peer to peer message to the shipper and describe the error 2. Send a verification request to the Mfr and upon response: a. VERIFIED: treat the product like a saleable return b. VERIFIED: automatically create a MediLedger transfer transaction c. NOT VERIFIED: indicate the product is suspect

In this scenario, the project group was relatively aligned on the systematic solution. Everyone believed that the seller should be automatically notified when the EPCIS file is missing, and that the trading partner should require verification in order to receive the product. In fact, there was concern over how the TI would be corrected and that it might make more sense to do a verification first since there is no TI to associate the product with at this point.

No.	Exception	Description	MediLedger
4	**Data, no Product @ Receipt**	**Received more data than products received.**	**Data, No Product during Receipt**

Conditions	Systematic Solutions
Shipment was short or never received EPCIS file was incorrect	1. Send a peer to peer message to the shipper and describe the error 2. Automatically create a MediLedger transfer transaction back to the manufacturer.

The project group was also very aligned on the response needed for Exception Scenario #4. The seller should be notified that there has been data received but no product, and that the system should automate a transfer back to the manufacturer of the extra serial number. The manufacturer (or upstream trading partner) will need to ensure that they are in possession of the product or investigate the missing product. The group stated that it will be difficult to reconcile to the level of SN at first due to packaging and other systems that would also need to be reconciled, but this will be required for the solution to fully function.

Suspect or Stolen Product Scenarios

One of the main goals of the DSCSA is to eliminate suspect stolen, counterfeit or otherwise harmful and counterfeit pharmaceuticals in the supply chain. The project group had three main goals in mind when identifying the following four suspect product scenarios and the systematic solutions to these suspect product scenarios.

- Identify suspect product in the supply chain
- Do not resell product that is suspect
- Distinguish between data errors for a legitimate product and a suspect product as quickly and clearly as possible

As noted above, exception handling scenarios could result in identifying suspect product also.

Four suspect product scenarios were identified, and the systemic solutions are included below:

- Duplicate serial number
- Product status is suspect/expired/recalled/destroyed/stolen
- Product with incorrect provenance
- GTIN doesn’t exist

No.	Exception	Description	MediLedger
1	**Duplicate serial number**	**Product scan shows the SN exists in two places**	**SN already exists**

Example:

- McKesson scans a product they believe has arrived from the manufacturer
- Notified by the MediLedger system that the same SN for that same product exists at FFF right now

Conditions	Systematic Solutions
1. Mfg or downstream trading partners introduces	1. Send a peer to peer message to the mfg for notification of duplicate SN 2. Send a peer to peer message to all custodians of the duplicate SN

duplicate SN 2. Error in data scan 3. Suspect product introduced into the supply chain	3. Mark this product as suspect

No.	Exception	Description	MediLedger
2	**Product status is recalled/destroyed/etc.**	**Product scan: previously recalled or has been destroyed, etc.**	**Bad product status**

Example:

- Cardinal Health scans a product upon receipt back from a retailer
- Notified by the MediLedger system that the product has a status of destroyed

Conditions	Systematic Solutions
1. Data issue 2. Product should be been recalled/destroyed but was diverted 3. Suspect product introduced into the supply chain	1. Send a peer to peer message to the mfg for notification of bad scan 2. Send a peer to peer message to the previous custodian of the product 3. Mark this product as suspect if it is previously recalled or destroyed

No.	Exception	Description	MediLedger
3	**Product with no provenance**	**Downstream trading partners scan product and find no previous transaction history**	**No provenance**

Example:

- Walmart scans a product and finds that there is no previous owner in the supply chain
- Notified by the MediLedger system that there is a provenance issue

Conditions	Systematic Solutions
1. Data error in scanning 2. Product sent to wrong trading partner, or trading partner down the chain 3. Suspect product introduced into the supply chain	1. Send a peer to peer message to the mfg for notification of no provenance 2. Send a peer to peer message to the previous custodian of the product 3. Send a verification request to the Mfr and upon response: a. VERIFIED: treat the product like a saleable return b. VERIFIED: automatically create a MediLedger transfer transaction c. NOT VERIFIED: indicate the product is suspect

No.	Exception	Description	MediLedger
4	**GTIN doesn't exist/isn't correct for the US**	**This GTIN does not exist in lookup directory or is not for the US market**	**No GTIN, bad GTIN**

Example:

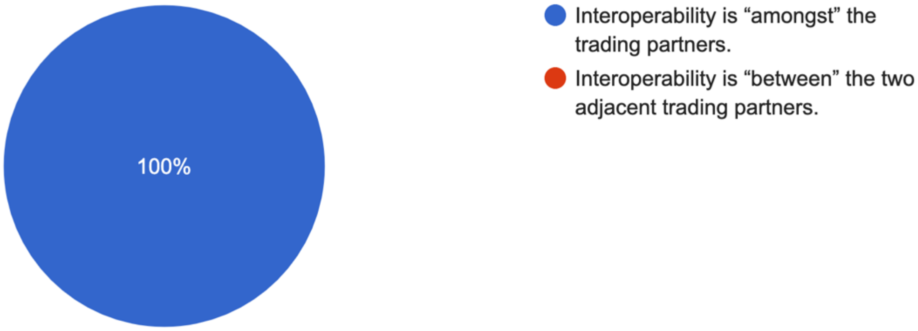
- Walgreens scans a product received from distributor
- Notified by the MediLedger system that there this GTIN does not exist in the system

Conditions	Systematic Solutions
● Data error in scanning ● Product is from another market ● Suspect product introduced into the supply chain	1. System to check for a 3 in the third position to ensure US product 2. Send a peer to peer message to the mfg for notification of no GTIN 3. Send a verification request to the Mfr and upon response: a. VERIFIED: treat the product like a saleable return b. VERIFIED: automatically create a MediLedger transfer transaction (How do we create then entire provenance?)

	c. NOT VERIFIED: indicate the product is suspect

System Adoption

The project held a workshop on system adoption and barriers to system adoption. We started with the definition of an “interoperable system” and the group was unanimous that the definition is amongst the trading partners, not simply between two adjacent trading partners.



In any interoperable system, it can be expected that all changes of ownership must be tracked in order to ensure a safe supply chain. The lack of full participation can ultimately create blind spots that can break the chain of custody. While the workgroup recognizes that a single entity owned system is unlikely and carriers with it some significant risks, there is also significant risk that data will become misaligned and incorrect as the number of interconnected systems grows. It is our belief that the key to success will require a well formed and FDA supported independent consortium to help the industry create aligned and effective standards of interoperability.

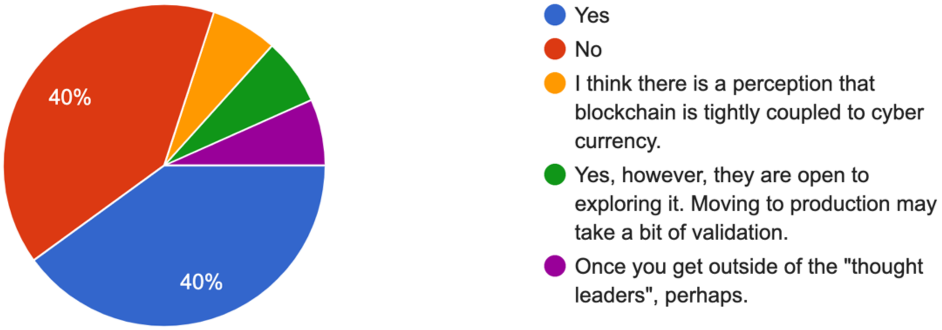
In discussing the barriers for full adoption, comfort with blockchain as a technology and data ownership were the main concerns. The second concern that arose was whether or not there will be full adoption by the industry. There are 1300+ manufacturers and 100+ distributors, and over 67,000 dispenser locations. The project group felt that critical mass would be achieved when 80 to 90% of the industry adopted the solution. The complexity of the network will mean that system adoption and system interoperability will be key to complying with the 2023 DSCSA requirements. Additional factors for full adoption are (in order of concern from most to least):

- System governance will be a challenge to work out (including system support between participants)
- Lack of clarity around interoperability
- Costs for smaller industry players
- Lack of standards across the industry
- Law does not require pharmacies to book returns
- System security
- A single system provider becoming a monopoly
- Expectation that enforcement dates will be pushed out
- Worldwide approach to verification/track and trace differs between regions
- Technical feasibly of actual different technology, and specifically blockchain network, interoperability

When considering which factors could contribute to increasing awareness of the requirements for track and trace, the following solutions were identified:

- More education to all parts of the industry (learning sessions, webinars, etc.)
- Prototype with well published results and benefits
- Engagement between all trading partners in the industry
- Establish a governance process
- Communication through industry forums
- Increased participation of dispenser segment

The group considered the question of whether or not there is a perception that blockchain technology is too “new”, and this may affect adoption of a blockchain solution. The group was split on the answer, with 40% believing that there is a perception that the technology is too new, while 40% felt that it is not a barrier to adoption. There is also an idea outside the blockchain industry that blockchain systems can be slow and cumbersome. However, with the architecture that was developed for the MediLedger Network, the system was designed to be scalable and very fast, avoiding the pitfalls of a system like Bitcoin.



There are also positive factors that will drive adoption. The group found the following characteristics will help the industry adopt an interoperable system (in order of importance from most to least):

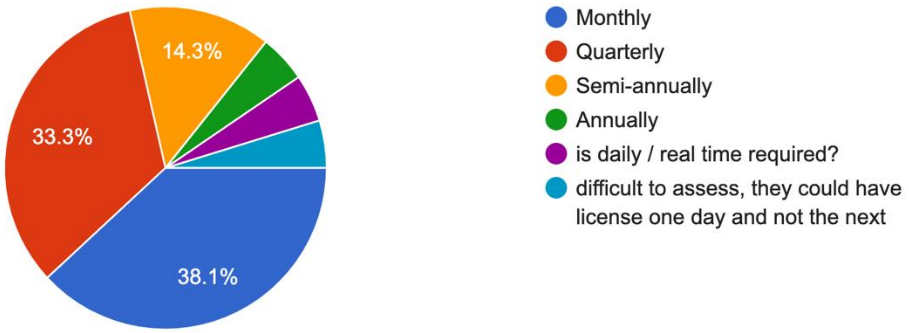
- Safety and security of the supply chain
- Creating an interoperable system for the industry can be the basis for future industry efficiencies
- Chargebacks simplification
- Supply chain optimization
- Process simplification
- Data marketplace for financial aspects of trade
- Improved system efficiencies
- Cold chain monitoring
- Cost and ease of implementation
- Immutable nature of blockchain
- Visibility to diversion that may have impact on return value from the manufacturer
- Recall visibility and management
- Reduction in inventory shortages due to improved visibility and forecasting

One important factor we considered was where the FDA could help to drive adoption and interoperability. The factor that received the most support was the desire for the FDA to share more about future expectations as early as possible, including governance. In addition, improved clarity around the regulations for the dispensing, disposal and end of life regulations for pharmaceuticals is very important. There is interest among the project participants that the track and trace requirements include all trading partners and not only legal owners. The non-legal owners that the group found would be the most useful to include in track and trace are reverse logistics organizations, CMOs, 3PLs, transportation providers, hospitals and even patients. 87% of our group felt that dispensers participating in track and trace is vital to making the system work effectively. There is a lot of concern around the lack of standards in the industry, and one suggestion was for the FDA to show support for a non-profit standards organization.

Authorized Trading Partners

To guard against distribution of counterfeit medicines, it is imperative that only authorized trading partners be able to access the MediLedger Network. The HDA has published a set of guidelines for identifying and monitoring authorized trading partners for VRS. While it is positive that we have a basic set of standards that can be expanded upon for a Confidential Change of Ownership system, the standards in this case are limited by the fact that there is no consistent way to identify authorized trading partners. Wholesale distributors are required to have state pharmacy licenses, though the requirements and processes for these vary from state to state. Manufacturers may have a Health Industry Number (HIN). Distributors have a variety of other identifiers like DEA number or 340B. The consensus of this group and the MediLedger DSCSA working group is that the only consistent way to identify all the members of the drug supply chain is for companies to attest that they belong in the network, gather at least one industry identifier from member companies, and then monitor that license or identification number over time. However, both groups are also very clear that if an industry identification number process existed, it would simplify many processes for them, including identifying and monitoring authorized trading partners. While it is valuable that we have requirements for VRS ATP, the group was in agreement that more requirements will be needed to meet DSCSA 2023 requirements. There are more business relationships in Confidential Change of Ownership than for VRS, and a more complex process than verifying product identifiers.

Once companies are identified and given access to the MediLedger Network, the group felt that monthly or quarterly monitoring would be the most useful. It is important to note that cross industry alignment is required in order to ensure security in a fully interoperable network so ultimately a newly established partner for DSCSA governance (such as that being suggested through PDSA) would be best to help drive alignment across systems.



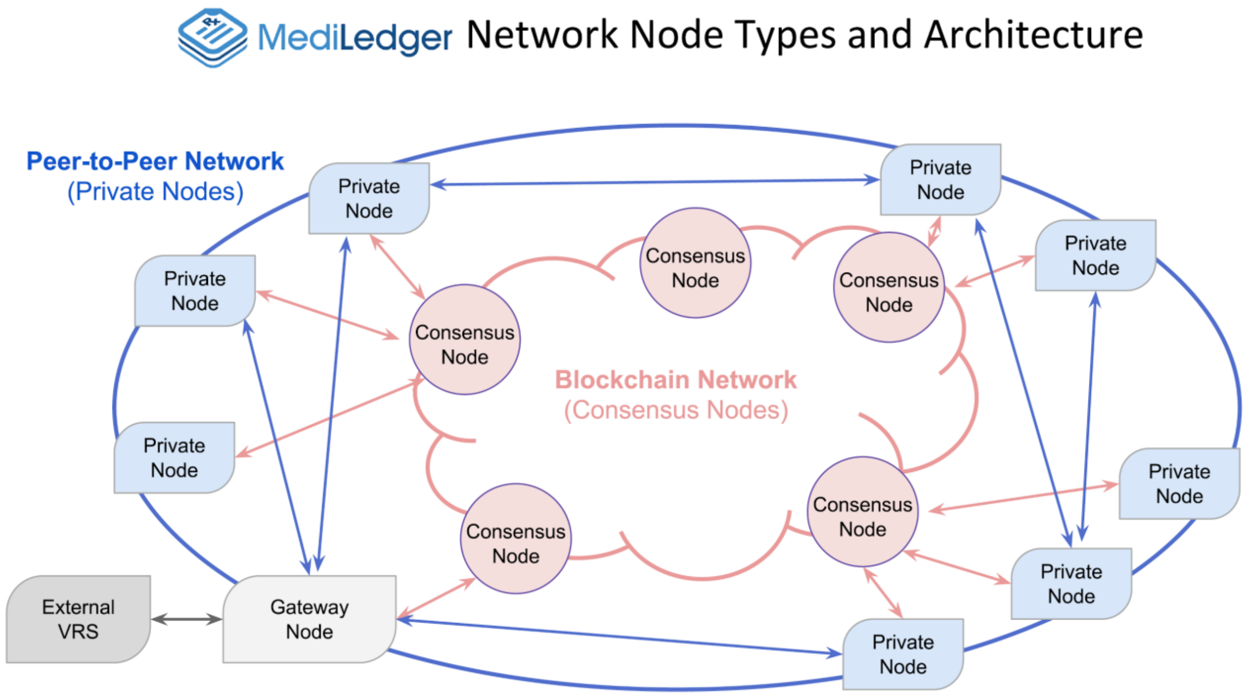
One topic we discussed in the project group was whether or not it would be helpful to move the ATP process to the blockchain to enable real time verification of authorization and create one source of truth for ATP. Some project group members noted that this would be helpful but questioned whether or not this needed to be real time and that we should be very careful about moving this process to the blockchain when it is still not fully established at this point.

Vision for Use of Blockchain

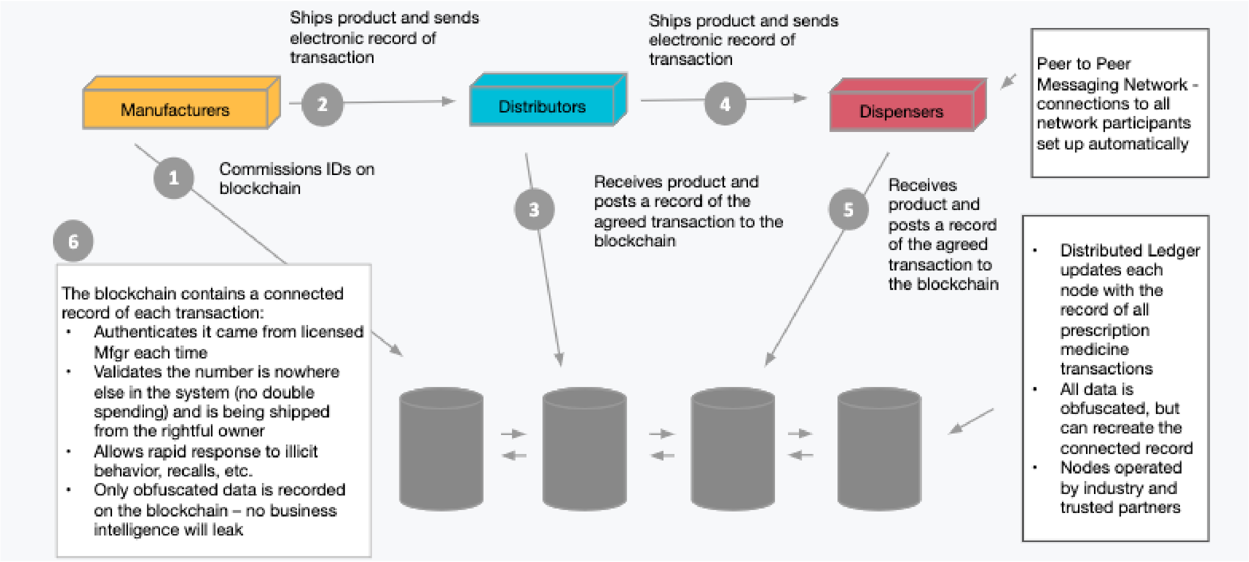
Solution Overview

At a high level, the overall MediLedger network architecture consists of Private Nodes that communicate peer-to-peer with each other as well as communicating with the blockchain through its own client that acts as a Consensus Node. The Consensus

Nodes form a blockchain network that is responsible for maintaining the blockchain data.



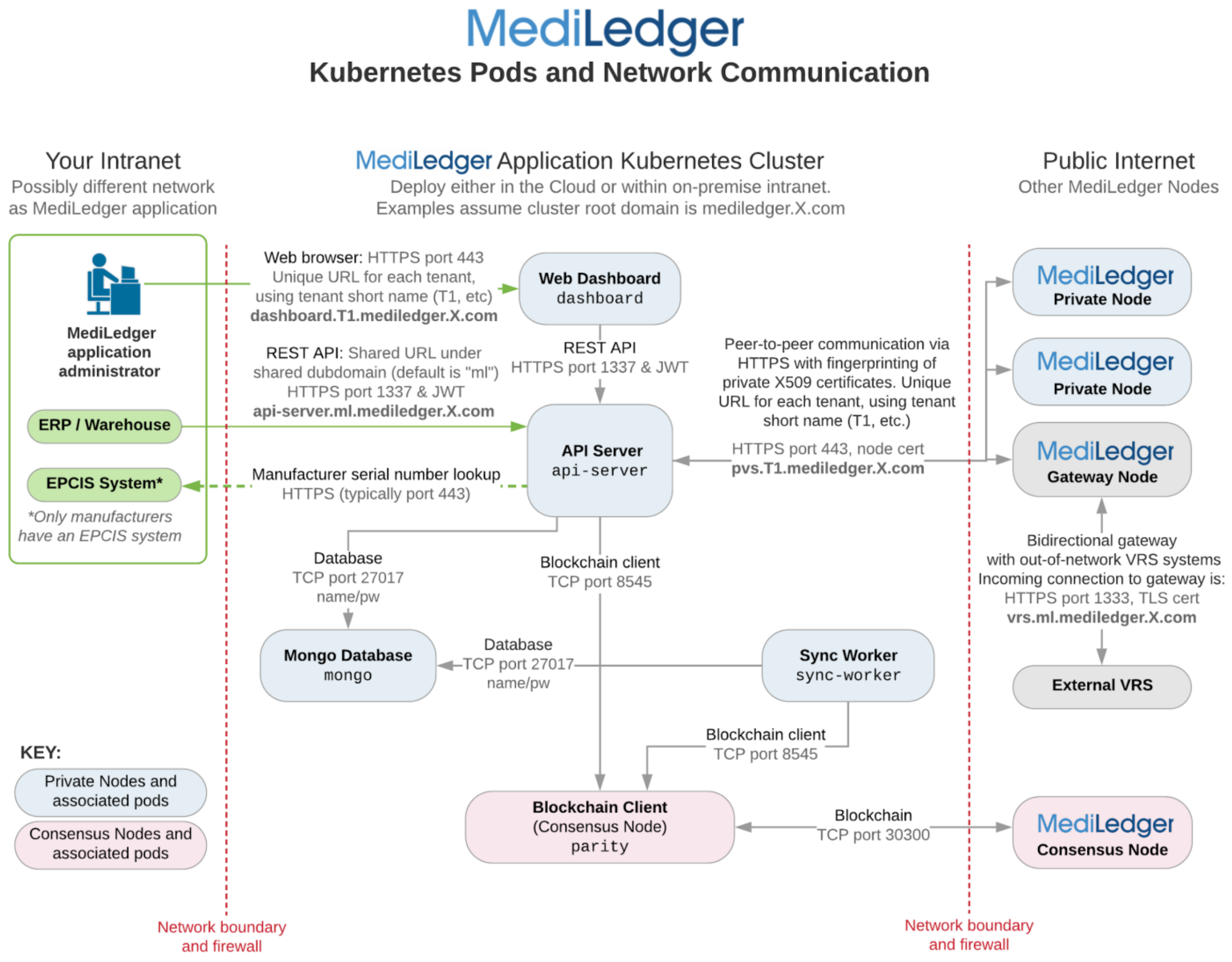
With such a network, we can create the capability of storing records of transactions on the blockchain, while allowing the exchange of electronic data, just as companies are expected to do today with the implementation of EPCIS messages. The power of the blockchain record is the immutable record of the change of ownership and the ability to have it check business rules that it is coming from the rightful custodian of that unit of medicine before finally being delivered to the rightful recipient. The power of the network is the ability to query participants as to the history of medicines that can respond with full provenance in a parallel fashion, rather than needing people to answer in series. This is critical to patient safety as it means near real time alignment on serial number status and location versus days or even weeks that may be needed for alignment with other types of solutions.


Ships product and sends electronic record of transaction
Ships product and sends electronic record of transaction
Manufacturers
2
Distributors
4
Dispensers
Peer to Peer Messaging Network - connections to all network participants set up automatically
1
Commissions IDs on blockchain
6
3
Receives product and posts a record of the agreed transaction to the blockchain
5
Receives product and posts a record of the agreed transaction to the blockchain
The blockchain contains a connected record of each transaction:
Authenticates it came from licensed Mfgr each time
Validates the number is nowhere else in the system (no double spending) and is being shipped from the rightful owner
Allows rapid response to illicit behavior, recalls, etc.
Only obfuscated data is recorded on the blockchain – no business intelligence will leak
Distributed Ledger updates each node with the record of all prescription medicine transactions
All data is obfuscated, but can recreate the connected record
Nodes operated by industry and trusted partners

A MediLedger network Private Node hosts multiple services:

- API server — This API server handles lookup request for a specific saleable unit. This provides REST APIs to separate systems (such as ERP applications) but also handles requests from other Private Nodes and even the Web Dashboard.
- For general API usage, this service uses a subdomain with the api-server prefix.
- If the request is coming from another Private Node, the request uses a different hostname (with a pvs prefix) with different port numbers and different authentication including fingerprinting of private X509 certificates.
- Web Dashboard — A web dashboard for the Private Node, which you can use to look up products (for distributors) or add GTIN product IDs (for manufacturers). This service is exposed with a subdomain with the dashboard prefix.
- Local Database — The internal database is implemented with the open source MongoDB software. It stores cached blockchain data as well as admin data for the Web dashboard.
- RabbitMQ — Messaging service.
- NGINX — Network proxy to manage incoming connections.
- Blockchain synchronization service — Every 5 seconds, this service calls out to the built-in blockchain client (Consensus Node) to get the latest updates from the blockchain. Finally, this service caches this data in the local database.
- Blockchain client (optionally running as Consensus Node) — When you install a MediLedger Private Node, the installation includes a blockchain client. In the MediLedger platform, the core software of the blockchain client is the open source software Parity, which is an efficient Ethereum blockchain client. The MediLedger network blockchain includes a list of manufacturers, a list of product IDs (GTINs) for each manufacturer, and a lookup directory of which MediLedger network Private Nodes handle a validation request for each product (specified by the ID known as a GTIN). The blockchain client can optionally run as a Consensus Node, which can help validate recent blockchain updates. Talk to Chronicled Support about whether you want your node to run as a Consensus Node on the network.

The solution is implemented using containers but can interoperate with other solutions via APIs:

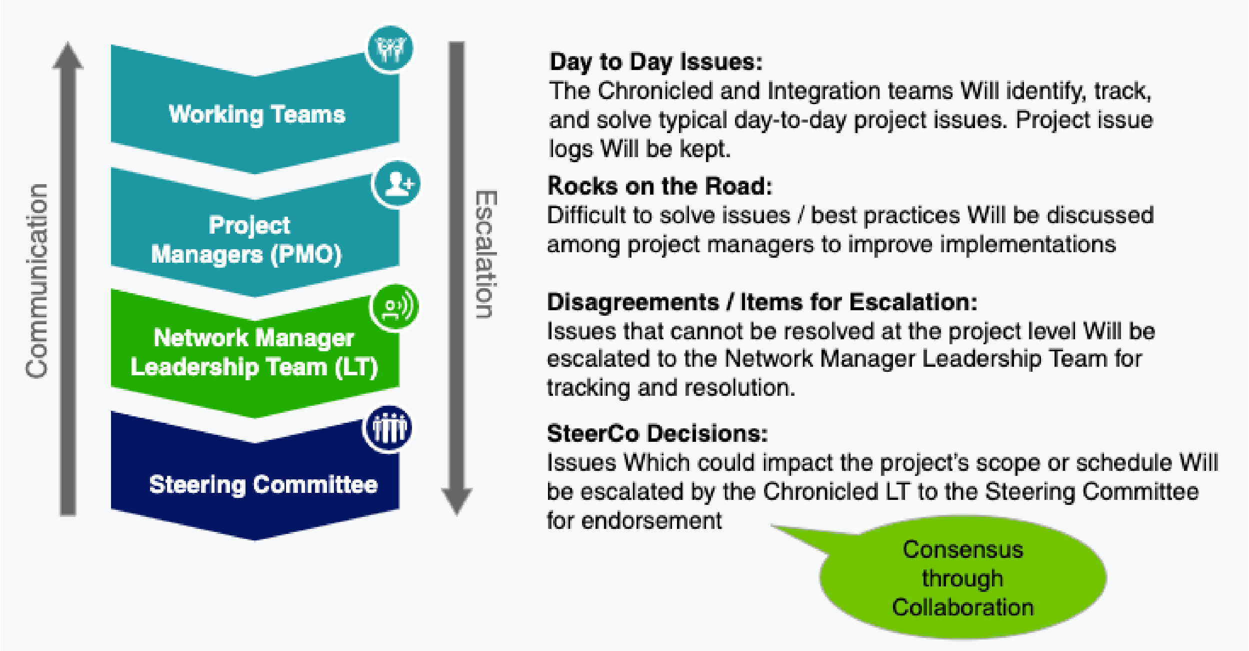


MediLedger
Kubernetes Pods and Network Communication
Your Intranet
Possibly different network as MediLedger application
MediLedger Application Kubernetes Cluster
Deploy either in the Cloud or within on-premise intranet.
Examples assume cluster root domain is medildeger.X.com
Public Internet
Other MediLedger Nodes
MediLedger application administrator
ERP / Warehouse
EPCIS System*
*Only manufacturers have an EPCIS system
Web browser: HTTPS port 443
Unique URL for each tenant, using tenant short name (T1, etc)
dashboard.T1.mediledger.X.com
Web Dashboard
dashboard
REST API: Shared URL under shared dubdomain (default is "ml")
HTTPS port 1337 & JWT
api-server.ml.mediledger.X.com
REST API
HTTPS port 1337 & JWT
API Server
api-server
Manufacturer serial number lookup
HTTPS (typically port 443)
Peer-to-peer communication via HTTPS with fingerprinting of private X509 certificates. Unique URL for each tenant, using tenant short name (T1, etc.)
HTTPS port 443, node cert
pvs.T1.mediledger.X.com
MediLedger Private Node
MediLedger Private Node
MediLedger Gateway Node
Bidirectional gateway with out-of-network VRS systems
Incoming connection to gateway is:
HTTPS port 1333, TLS cert
vrs.ml.mediledger.X.com
External VRS
Database
TCP port 27017
name/pw
Blockchain client
TCP port 8545
Mongo Database
mongo
Database
TCP port 27017
name/pw
Sync Worker
sync-worker
Blockchain client
TCP port 8545
Blockchain Client
(Consensus Node)
parity
Blockchain
TCP port 30300
MediLedger Consensus Node
KEY:
Private Nodes and associated pods
Consensus Nodes and associated pods
Network boundary and firewall
Network boundary and firewall

Guidelines for Governance

We are driven by the MediLedger Network guiding principles which put industry first, ensure equal access, and ensure the privacy of individual company's data. As such the governance of the network will follow these same guidelines. The governance body is accountable for the interests of the entire network, and is responsible for making policies, rules of conduct and operating procedures. In addition, governance will address how the group will avoid anti-trust conflicts. Network participants will be members of the governing body, if they so wish. The goal of the governing body is to achieve consensus through collaboration, rather than members having specific voting rights. In the event consensus cannot be achieved, the first approach is to modify the solution design to push unique requirements to company controlled private rules, leaving rules that all members can agree upon to be codified in the blockchain. This methodology has been very successful since the beginning of the MediLedger Project in 2017.

When discussing governance with the project group, there was strong interest in having industry participate in the governance, and especially if the solution is a blockchain solution. With a blockchain based solution, the solution is distributed, and the infrastructure is owned and run by the industry. The project groups emphasized that in this situation, industry participation in governance, or industry led governance, will be key.



Day to Day Issues:
The Chronicled and Integration teams Will identify, track, and solve typical day-to-day project issues. Project issue logs Will be kept.

Rocks on the Road:
Difficult to solve issues / best practices Will be discussed among project managers to improve implementations

Disagreements / Items for Escalation:
Issues that cannot be resolved at the project level Will be escalated to the Network Manager Leadership Team for tracking and resolution.

SteerCo Decisions:
Issues Which could impact the project's scope or schedule Will be escalated by the Chronicled LT to the Steering Committee for endorsement

Blockchain Interoperability

Today's limited landscape of blockchain solutions are not interoperable. This means that one blockchain has no knowledge of information that might exist in a different blockchain. Using crypt as an example, the Bitcoin (BTC) blockchain exists fully independently of the Ethereum (ETH) blockchain — in the sense that it has no knowledge of any information recorded there — and vice versa. Blockchain-based projects are isolated from each other, despite their attempts to support the same industry and working with the same technology.
The MediLedger presumption is that there will be multiple blockchains which support single business requirements (comply with DSCSA), as well as other blockchain solutions which would benefit from integration and interoperability.

The conclusion also includes the idea that there will be multiple base layer blockchain ledgers which will need to be interoperable (Ethereum, Hyperledger Fabric, Etc.…)

As the need to have different blockchain solutions talk to each other grows, there are a number of projects focused on this problem (Reference: cointelegraph article)

Polkadot
Polkadot is a multichain, or cross-chain, technology. Basically, it allows different blockchains to plug into a larger, standardized ecosystem. It was founded by Gavin Wood, a co-founder of Ethereum.

Technically, Polkadot is comprised of parachains (i.e., parallel blockchains that process transactions and transfer them to the original blockchain), a relay chain (i.e., a central component that connects parachains and ensures their security), and bridges that connect Polkadot to external blockchains.

Cosmos
Cosmos also follows the cross-chain principle. Specifically, it employs an inter-blockchain communication (IBC) protocol to establish blockchain interoperability. It serves as a TCP/IP-like messaging protocol for blockchains. Since various established blockchains (like Bitcoin) do not support IBC by design, Cosmos uses the so-called "peg zones" to connect them to the "Cosmos Hub" — as the project is called — a "flagship" blockchain that binds all the zones together and coordinates communications between them via standardized languages.

However, the Cosmos Hub is a part of the larger interchain ecosystem developed by Cosmos that can contain other entities — for instance, there is also Iris Hub, which focuses on enterprise customers and Chinese clients.

Chainlink
Chainlink is a decentralized Oracle service. It allows for data to be retrieved from off-chain APIs and be put on a blockchain. In other words, Chainlink serves as a bridge between blockchains and all the infrastructure that exists off-chain: Oracle

nodes receive real-world data, process it through the network and take it to the blockchain. Notably, the company cooperates with the global interbank data transfer and payment system SWIFT, used by most banks across the world.

Wanchain
Wanchain uses a different protocol to facilitate data transfers between otherwise unconnected blockchains. Thus, instead of deploying peg zones or its multichain analogs, Wanchain creates so-called “wrapped” tokens that can be traded on other blockchains.

For instance, to move 10 ETH to the BTC chain, the platform would first lock that amount of ETH on the Ethereum blockchain using smart contracts, which would then mint 10 Wanchain-wrapped ETH (WETH) on Wanchain. These WETH could then be traded for Wanchain-wrapped BTC (WBTC) on a trading platform. Those wrapped BTC tokens can then be turned into the original tokens located on the Bitcoin blockchain.

Quant
Unlike the aforementioned examples, Quant is not a blockchain. It uses Overledger protocol, a layer that runs over existing blockchains. Overledger ostensibly allows developers to create “MApps” — decentralized applications (DApps) that utilize multiple blockchains at the same time — in “three lines of code” and without any additional infrastructure. That allows for more options in blockchain engineering. For instance, an MApp could rely on the Ethereum blockchain for data storage while using Bitcoin Cash (BCH) for value transfer.

For pharma blockchain interoperability to be successful, it would require alignment around basic tenets. Such as:

- The ledger is not a general-purpose DB. While the blockchain can store some data, it is too expensive to store ‘regular business data’ across dozens or hundreds of nodes at scale. The blockchain should be used sparingly when and only when it contributes value to the enterprise solution stack.
- The base layer blockchain ledger should only be used to perform services where it has a natural comparative advantage over other technologies. Using the base layer technology for purposes where it does not have an advantage is like using a frying pan for pounding nails or a hammer for frying eggs. For blockchain, the areas where it has a natural advantage includes serving as a system of record for regulatory record-keeping, master data synchronization, digital asset exchange, business rule enforcement, and decentralized multi-enterprise business process automation.

Summary/Next Steps

The **MediLedger FDA Pilot Project** has shown that it is feasible to use a blockchain based solution for compliance with The Drug Supply Chain Security Act (DSCSA) requirements related to the interoperable, electronic tracing of products at the package level.

Based on business requirements and guidance from our project team, we developed a blockchain-based system for tracking the legal change of ownership for prescription medicines, and we have drawn the following conclusions:

- Industry stakeholders currently use the GS1 Standard Electronic Product Code Information Services (EPCIS) solution (level 4 system) to meet the DSCSA mandates. Through this project, we have shown that blockchain has the capability to be the technology underlying an interoperable system for the pharmaceutical supply chain, as mandated by DSCSA. When using a single blockchain solution, transaction throughput, speed, and reasonable cost can be achieved to meet stakeholder needs.
- Data privacy requirements of the Pharma industry can be met using "*zero knowledge proof"* technology, where all transactions posted to the blockchain are fully obfuscated, ensuring no confidential information or business intelligence is shared. The design allows for nodes in the blockchain system to be hosted by multiple unique parties while maintaining strict transactional privacy and still ensuring immutability of the transactions.
- A blockchain system can be capable of validating the authenticity of product identifiers (verification) as well as facilitating the provenance of saleable units back to the originating manufacturer.
- The authenticity of the drug transaction information can be confirmed with each transaction allowing for expedited suspect investigations and recalls.
- The group believes that should a blockchain ecosystem be created as a possible solution to the DSCSA interoperable solution requirement, it should have an open system architecture with an appropriate governance to oversee the function of the system and ensure compliance with industry agreed business rules and standards of operation.
- Governance should come from the industry itself
- The trust established by a blockchain system can be leveraged for a myriad of additional business applications to the pharmaceutical industry, allowing for compounding benefit for this industry once such a platform is established.
- As we see from every step of implementation of DSCSA, this is a complex solution that will require a stabilization period. The implementation date and the FDA enforcement date could be separate and planned in advance.
- The long-term success of a truly interoperable blockchain-based solution will require strong participation and adoption from all industry stakeholders (manufacturers, wholesalers, dispensers, service providers, etc.).
- There are clear challenges with making disparate track and trace systems interoperable. The project group is concerned that no standards currently exist to make

the multiple systems interoperable, and without appropriate standards, it is not likely that disparate systems can be made successfully interoperable.

As for next steps, the group identified a number of factors that would increase the chances of success in implementing the 2023 DSCSA requirements. First, there are at least four sets of standards that still need to be developed; messaging (EPCIS updates), system interoperability, APIs, and authorized trading partner identification. The group is also very clear that implementation and usage throughout the industry will be simplest if the industry uses a single neutral platform for track and trace, one that ensures confidentiality and trust throughout each step of the supply chain.

In general, there are a number of industry problems which are the result of inefficiencies between trading partners, failures in cross-company communication, and the reliance on antiquated technology which is used today to exchange information. Protocols which utilize blockchain can be established that groups of companies benefit from participating in together, enabling enforcement of cross-industry business rules. The vision is that these protocols are not in principle controversial agreements; on the contrary, they simply put in place the pipes that allow industry improved capability and reduced friction to do business with their trading partners in any way they best see fit. Compliance with DSCSA is just one use case.

There are recurring patterns where the MediLedger Network with blockchain-components can add value in the context of a multi-enterprise business network:

- **Data Synchronization**- The use of a blockchain as an industry utility for accuracy and completeness of data files. The Synaptic Health Alliance’s provider directory data sharing initiative is an example of this design pattern. Proof of Authority (PoA) consensus creates strong guarantees around master data synchronization.
- **Asset Exchanges**- The use of a two-sided market for the exchange of digital assets that have value for buyers and sellers / curators. Product identifiers serve both as digital IP and as an endpoint in an operational messaging so that they can actually be transferred under the M&A scenario when a seller sells a molecule to the buyer without interrupting the operational performance of the system.
- **Multi-Party Business Process Automation**- The foundational use of a shared source of truth between transacting parties in a business process for the purpose of automation, operational intelligence, and model innovation. A decentralized business process for sending and responding to drug verification requests means that hundreds of companies can participate in a mostly closed loop process that upgrades trust and security in the supply chain in an automated and efficient format.
- **Business Rule Enforcement**- With zk-snarks plus smart contracts, we can use the blockchain as a neutral regulator, inspector, or enforcer of industry-wide regulatory rules and business rules. For example, we can create a rule like, “only Mfg A is allowed to commission or send SGTINs containing Mfg A’s company

prefix” or “an SGTIN can only move forward in the supply chain if it originated from a licensed manufacturer and if all prior transfers between trading partners on the network followed the rules and were valid. Used in this way blockchain plays the role of an army of tens of thousands of clipboard carrying inspectors, inspecting and approving every transaction, to ensure that the letter of the regulation is followed. What’s even more exciting is that with zk-snark we also gain the benefit of 128-bit encryption applied to the payload of every transaction which proves to be a very strong data privacy solution also.