# A Solution for Pharmaceutical Track and Trace in the United States - Part 2

*This article is Part 2 of a four-part series on solving the Track-and-Trace requirements being faced by the participants in the US pharmaceutical supply chain. Part 1 describes current industry efforts to define a solution that meets both regulatory and business requirements. Part 2 provides a high-level description of a new solution that relies and leading edge technology that has been proven over ten years of rigorous practical use. Part 3 describes the step-by-step choreography of the new solution. Part 4 describes the characteristics of an Independent Administrator to oversee the solution on behalf of all stakeholders: industry and government, alike.*

In part 1 of this series we briefly described the requirements of the Drug Supply Chain Safety Act (DSCSA) and the state of current efforts to address the requirements for the Track and Trace portion of the DSCSA. In this article, we present a novel approach that appears to meet the Business, Legal, and Technical (BLT) requirements of all of the supply-chain-stakeholders.

The current model imagined by the industry requires each member of the supply chain to manage its own data which includes identification of both their sources for products purchased and their customers for products sold. In order for the FDA (as well as other law enforcement) to be able to track a product that goes through multiple supply chain members is to concatenate the data from a manufacturer with that of a distributor, as well as any other parties included in the supply chain (e.g., re-packagers). This solution is complex, insecure, and expensive.

In the remainder of this installment, we describe a new, alternative solution that addresses all of the critical requirements of both the FDA and the industry[i]. The solution is simple, secure, and inexpensive. We compare the two solutions in Table 1.

**Table 1: Comparison of Current and New Solutions. New solution addresses all of the requirements of DSCSA and all of the features of the current solution, but adds *Dynamic Detection*™ of suspicious transactions, low cost, and increased security.**

| Category | Feature | Current Solution | New Solution |
|---|---|---|---|
| **Technical Solution** | Supports the tracking of a product's transaction history to its source to verify its provenance | Yes | Yes |
| | Supports tracing of a product through the supply chain for purposes of a product recall | Yes (slow)<br>System may have difficulty dealing with lack of certainty about which Serial Numbers are included in each carton, making the tracing of a particular | Yes (near real-time) |

| | | | |
|---|---|---|---|
| | | package difficult | |
| | Supports dynamic identification of questionable transactions | No | Yes |
| | Visibility of transaction data to other supply chain members | Information is available only to parties directly involved in a transaction | Information is available only to parties directly involved in a transaction |
| | Easy integration of transaction data across the supply chain | Maybe<br>Integration of data from a multiplicity of different databases with different underlying schemas, database products, and maintenance schedules | Yes |
| | Support tracing product through supply chain when Serial Numbers are imprecise | Maybe | Yes |
| | Number of separate databases required | Thousands<br>At least, one per company | 1<br>Single database replicated in multiple locations for security |
| | Number of Identity and Access Management systems required | Thousands (One per company) | 1 |
| | Scalability (more companies) | Infinite, significant impact on complexity | Infinite, negligible impact on complexity |
| | Scalability (more products) | Infinite | Infinite |
| | Scalability (more transactions) | Infinite | Millions |
| **Business Solution** | Database structure | Requires each firm to establish its own tracking database | Single, shared solution |
| | Identity and Access Control | Requires each firm to establish a vetting and access control mechanism for the database | Single, shared solution |
| | Firms control their costs | Cost will be high and open-ended | Costs will be low and fixed |
| | Cost fairness | Costs will be disproportionately high for small firms | Costs can be tiered to accommodate smaller firms |
| **Security** | Ease of access by regulators/law enforcement | Difficult<br>Authorized agents (e.g., FDA, law enforcement) may need to obtain access credentials to access each of the hundreds of different databases | Easy<br>Single point of access to all data |
| | Resistance to collusion | Medium | High |

| | | | |
|---|---|---|---|
| | Resistance to data alteration | Medium | High |
| | Resistance to breach | Low-Medium | High |

As can be seen from the table, the new solution is more simple, more secure, and more cost-effective than the current "de-centralized database" solution.

## High-level description of the new solution

The new solution collects all of the supply chain's transaction data in a single database. But the entire database is encrypted so that its data are not visible to members of the supply chain, nor are they usable to any hacker who seeks to breach the system. The data integrity is maintained by requiring digital signatures of both seller and buyer before a transaction is recorded in the system. And the database is replicated in multiple, disparate locations, so that if a hacker is able to breach a single copy of the database and altered it, the change would be recognized by a consensus of the other copies and that version of the database would be rewritten to conform to the consensus.

The technology underlying this solution is known as blockchain. It is the technology that underlies Bitcoin and has successfully protected the $8 billion Bitcoin ecosystem for nearly a decade. (While Bitcoins value has been volatile, the underlying blockchain technology has never been broken.) This technology is so powerful that major banks including Goldman Sachs, JP Morgan, Credit Suisse have been investing millions of dollars developing solutions for their industry.

Essentially, the blockchain is an encrypted transaction log. It tracks every transaction to ensure that transactions a valid, accurate, and non-repudiatable. And because of the unique encryption used in the blockchain the data are masked -- even though the database itself may be freely viewable and auditable.

Once a log of all transactions is created, it becomes easy to perform the three key functions required by DSCSA:

1. identify the path a drug took to get to its present place in the supply (including its ultimate manufacturing provenance)
2. identify all current holders of a product undergoing recall in order to issue recall notices to them (without having to disclose the downstream path to the manufacturer issuing the recall)
3. *Dynamic Detection*™ of suspicious transactions.

Tracking the path through which a drug propagates through the system is merely a matter of using the transaction data to create a giant input-output table which includes a series of counters for every member of the supply chain to track their inventory of every product that they handle as illustrated in Figure 1.

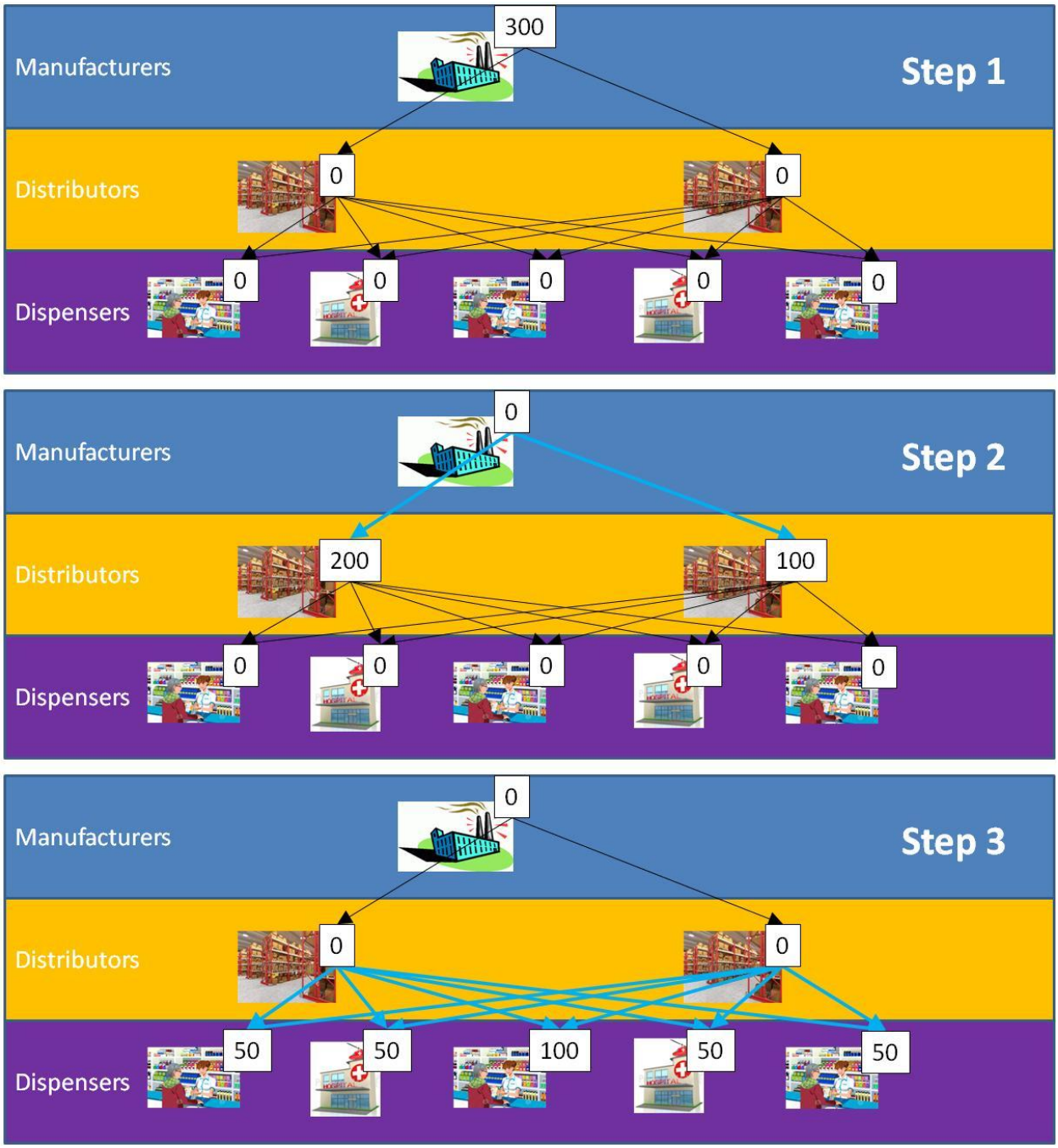


**Figure 1: Change of Ownership Tracking. By tracking the input and output flows from each member of the supply chain, "the system" is able to maintain visibility of the path of dissemination of a particular product to recognize which parties have how much inventory. But individual supply-chain members can only see their immediate upstream and downstream transactions.**

In Step 1 of the figure, a manufacturer commissions 300 units of a new product. All downstream counters are at 0 because they have no inventory of the new product.

In Step 2 of the figure, the manufacturer sells 200 units of the product to Distributor A and 100 units to Distributor B. Accordingly, his counter decrements to zero and the 300 units are now spread among Distributors A and B.

In Step 3 of the figure, Distributor A and Distributor B sell all of their product to Dispensers D, E, F, G, and H. Each transaction updates the blockchain database and the entire dispersion pattern of the drug (via the counters) is updated with each transaction. This allows "the system" to know where all of the product is at any point in time. This not only allows regulators to track the path of any product back through the supply chain, but it also allows for the ability to trace forward to identify all holders of the product during a recall. In a recall, the manufacturer can submit a notice to "the system" and it will propagate the notice to all identified holders of the drug in near-real-time without the manufacturer having to be granted visibility to his supply chain downstream of its own customers.

### *Dynamic Detection™*

A particular advantage of this solution is *Dynamic Detection*™: the ability to dynamically identify suspicious transactions as illustrated in Figure 2.

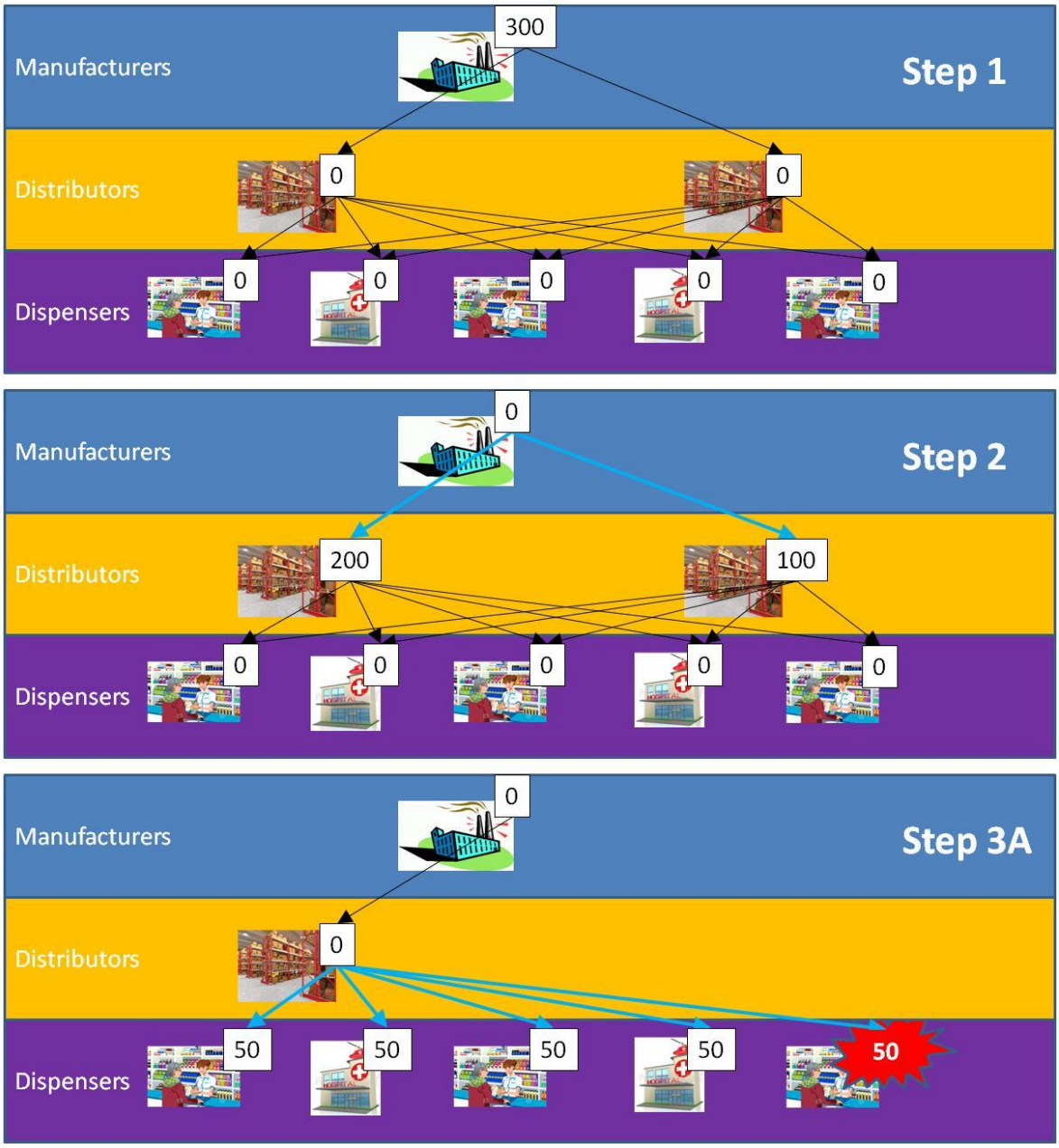


**Figure 2: Dynamic Detection of Suspicious Transactions. Because the solution can ascertain the net inventory of legitimate product at any point in time, it can detect suspicious transactions: when a firm sells more products than it has received. It can even prevent such transactions from taking place.**

In this figure, Steps 1 and 2 are identical. But in Step 3A we highlight Distributor A's attempt to introduce counterfeit, gray-market, or diluted product into his downstream supply chain. The transactions to Dispensers D, E, F, G, and H occur in the order of time. By the time the Distributor has sold 50 units to the first four Dispensers, his inventory is at zero. He no longer has product to ship to Dispenser H. Accordingly, this transaction will be flagged.

It could well be the case that the product shipped to Dispenser H is legitimate and that the Illegitimate product was shipped to a different Dispenser. But as soon as the Distributor A tries to sell more than he has, all his transactions of the product become suspicious and the FDA and/or law enforcement can be alerted.

One of the benefits of this solution is that it can be configured to prevent the last transaction from occurring. In this way, there will be no way for Distributor A to even attempt to create a paper trail in which he sells more than he has. This further reduces the incentive to cheat. For, even if he purchases Illegitimate products, he will never be able to sell more product than the amount of legitimate product he has purchased. Assuming, for simplicity that he possesses 200 legitimate units of a product that he sells for $10 each, he will never be able to receive more than $2000 ($10*200 units). If he sells 100 legitimate packages and 100 Illegitimate product packages, he will receive the same $2000 and have another 100 legitimate units in inventory. But he will be unable to sell these because as soon as he tries to sell unit 201, the transaction will be flagged. The legitimate product will be left to expire in inventory.

### Serial Number Independence

Another benefit of the solution is that it is not dependent on serial numbers. Because the system is based on volume, it can detect Suspect product transactions even when they use legitimate (counterfeit) serial numbers. This diminishes the importance of randomizing serial numbers. If a counterfeiter creates products with legitimate numbers, he cannot introduce them to the supply chain without creating a surplus of product. If Distributor A duplicates the serial numbers in his inventory and sells legitimate product to one Dispenser and Illegitimate product to another Dispenser with the same "valid" serial numbers, the transactions will be flagged for exceeding his inventory or legitimate product.

### Imprecise Serial Numbers

This volume basis also accommodates the difficulty that manufacturers and repackagers may have in "certifying" the precise serial number contents of cartons and/or pallets. The solution is robust enough to allow the serial number data included in a transaction reference a batch of serial numbers. As the cartons are broken down while the products traverse the supply chain, the system can even replace the batch reference with specific numbers.[ii]

## Economics

As a shared solution managed by a Solution Provider, the costs of the new solution can be spread across the entire supply chain, making it cost-effective. And as a shared solution, fixed pricing can be established for each supply chain member. And this pricing can be tiered so that larger companies with more products and more transactions can be placed in one tier while smaller firms can be placed in another to ensure fairness and enhance participation. An Independent Administrator (to be established) defines the rules for pricing. This may mirror the current industry model illustrated by the SAFE BioPharma Association which manages the identity credentialing process for the industry on a global basis.

## Security

A top priority for the members of the supply chain is ensuring the confidentiality of the proprietary transaction data that is contributed to the database for track-and-trace purposes. The solution achieves this through encryption. Each transaction recorded in the system is digitally signed by both the seller and the buyer. Once each party reviews and agrees that the transaction is accurate, their signatures are used to encrypt the data in the blockchain database. A single system (e.g., SAFE BioPharma) can be used to issue identity credentials and encryption keys to each authorized party.

Once data are appended to the encrypted transaction log, it can be viewed only for audit purposes by authorized independent auditors selected by the Independent Administrator.

For other users, data will only be obtainable through standardized reports. Users do not directly touch the database after approving and digitally signing a transaction. The Independent Administrator establishes the format for reports and the rules of access that limit who can obtain reports on particular transactions. Reports limit industry members to accessing data only for which they were one of the transacting parties (except for a report providing the name of ultimate manufacturer of a particular package).

The database is also replicated after every transaction in multiple locations. This not only reduces the possibility of data loss due to disaster, it also means that a hacker -- were he able to interpret the encrypted data -- would have to simultaneously make the same changes to multiple versions of the database to propagate bad data. Because the database Is being updated continuously, this is unlikely.

---

[i] The alternative solution has been developed by Rocky Mountain Technical Marketing. (See http://www.rmtminc.com/.)

[ii] In current practice in the US, this is not likely to happen because DSCSA does not require final sales by Dispensers to be recorded. This is the only place where specific numbers would be identified.