CENTER for Supply Chain Studies™

ReferenceModel-based Exploration and Education

Executive Brief

THE VALUE OF BLOCKCHAIN

AND ITS APPLICATION TO THE

DRUG SUPPLY CHAIN SECURITY ACT

Prepared by:

Robert Celeste, Founder
Center for Supply Chain Studies
February 5, 2018

CONTENTS

INTRODUCTION

As with most new innovations, blockchain has experienced its fair share of hype, myth and misunderstanding in the general population. It's both lauded by a development community that sees its unfettered use, yet closely scrutinized by a highly regulated industry in need of responsive, secure, stable and risk-free systems. As history has shown us, there is often a wide gap between the imagination for innovation and the reality of business and regulatory requirements.

Based on the nature of our complex and ever-evolving business needs, blockchain as a *technology* continues to mature and transform. Most importantly, it represents an opportunity to break from the current mindset of transaction processing to a more fluid atmosphere of autonomous agreements, information discovery and responsible management of sensitive information.

Blockchain platforms offer a place for simplified electronic connections between parties, data integrity, programmability, visibility, security and confidentiality – all features of an *effective environment* where trading partners can securely exchange data while automating business and regulatory rules. These are also the features of an interoperable and secure system called for in the Drug Supply Chain Security Act (DSCSA).

OBJECTIVES

The purpose of this brief is two-fold:

1. To provide a non-technical audience with a *clear explanation* of blockchain technology and its possible benefits, including compliance with the DSCSA, new business opportunities, etc.
2. With this knowledge in hand, enable this audience to *confidently* explore blockchain options.

A MISUNDERSTANDING

Understanding blockchain is often difficult at first. News articles and other presentations frequently mix information about blockchain concepts with platform capabilities. The result is an observer left believing that all blockchain platforms have the exact same set of capabilities, components and names.

For example, blockchain platforms like Bitcoin, Ethereum, Hyperledger and others make use of blockchain concepts by adding other features to facilitate the purpose of their platforms. This may include exchanging currencies, transactions and documents, or functioning as a general application development environment.

Later in this brief we provide further explanation of the differences and distinctions of blockchain concepts and blockchain platform capabilities. However, it is important to first identify a few basic concepts before understanding how specific blockchain platforms add these concepts to create their own unique capabilities.

THE CHALLENGE FOR PHARMA

The 2013 Drug Supply Chain Security Act prescribes a set of compliance requirements for pharmaceutical supply chain participants over a 10-year period (2013-2023). Most notably, it requires manufactures of pharmaceutical products sold in the U.S. to serialize, or uniquely identify, the 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 supply chain participants are required to put into 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). This could amount to tens of thousands of electronic connections between previously "unknown" entities. Because most current trading partner transactions are typically between known trading partner pairs, the new challenge of "instant trust" has emerged.

Currently, no such electronic system exists.

IS BLOCKCHAIN THE SOLUTION?

Blockchain technology and its platforms provide some hope in that current digital platforms such as Bitcoin, Ethereum and others have successfully demonstrated the capability to establish a trusted, secure exchange of currency or information between "heretofore unknown parties" that may address the challenge of an "interconnected system" called for by the DSCSA.

BLOCKCHAIN CONCEPTS

Blockchain as a concept is relatively simple, but does include some complex features like cryptography, Merkle trees, proof-of-work, hashing and others that may seem confusing to a non-technical person. However, like our cell phones, there's no need for us to understand their electromagnetic wave propagation or data packet management systems to operate and appreciate them. The same is true for blockchain.

There are two main concepts that are native and integral to blockchain platforms that are extremely helpful to further grasp and appreciate the value of blockchain implementations – they are *data integrity* and a *distributed network*.

1. **Data integrity:** This is often also referred to as data immutability, or the ability to ensure that a given set of data cannot be changed or removed. Blockchains accomplish this by *grouping* posted transactions as a "block." Each block is assigned a block identifier (ID). Additional transactions are gathered into the next block and the block ID of the previous block is included in this new block (and so on). This is what establishes the continuous link (or chain) between a series of blocks – hence the name "*blockchain*".

To ensure the data is tamperproof, a calculation is performed on each block of transactions, resulting in a fixed series of characters that can only be created from that exact block of data. This series of characters is referred to as a *hash value*. Any change to the original data, even an additional space, would result in a different hash value.

The hash value for the previous block is included in the current block. Therefore, the removal of transactions (or blocks) within a chain will also result in a different hash value than the one stored in the next block making it *impossible to tamper* with data in any block without detection.

This is especially important in context to the DSCSA because it allows supply chain partners to post information on a blockchain that may be needed by unknown (but legitimate) members of the supply chain. This helps to bolster trust between trading partners by assuring that data cannot be manipulated or removed.

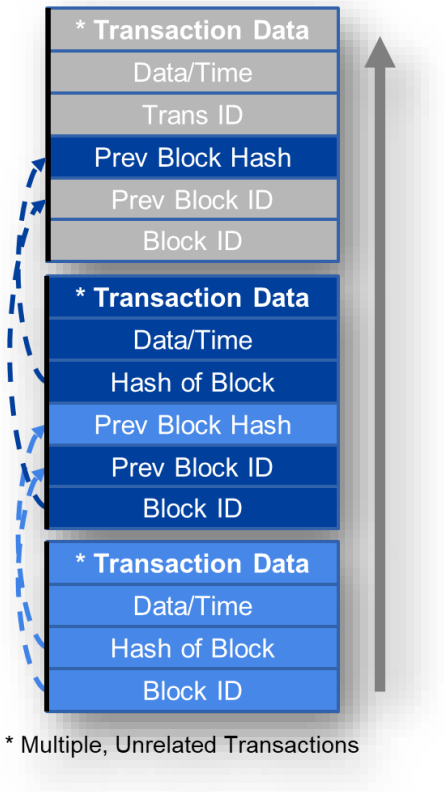

Figure 1 - *Blockchain Data Integrity Concept*

2. **Distributed network:** To allow electronic access to blockchain data and further protect against tampering, blockchains are implemented on a *distributed network of connected computers*. Called "nodes," these computers are utilized to protect against failure of any one node and, without exception, ensure that *all nodes hold the exact same set of data*. There is no central system or computer that orchestrates the behavior of the nodes. Rather, there is a *shared protocol* within which each node complies to correctly verify and distribute data.

   The job the node is to ensure that all nodes agree upon what data makes up the legitimate blockchain and share that data with each other. If a node *does not* reflect the exact same data set as all other nodes, that "offending node" data is not incorporated into the legitimate, shared data set. Although there are multiple copies of the blockchain, this note utility ensures that there is only one true set of data and provide multiple secured access points for industry participants to connect.

   This is also important in context to the DSCSA in that the tens of thousands of potential supply chain participants can connect (via the nodes) to the blockchain data (granted certain access rights). Along with block hash values, node consensus also protects the integrity and availability of the true data set (blockchain).

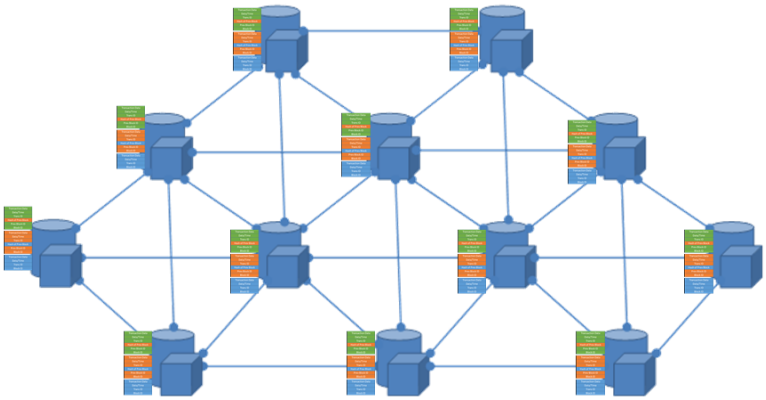

Figure 2 - *Identical copies of blockchain data held on each node*

BLOCKCHAIN PLATFORMS

Blockchain concepts are implemented and enhanced in blockchain platforms. Managed by consortiums and solution providers, these platforms regularly add new features and functions to meet new consumer demands, including data storage and lookup, distributed applications and other. Based on their user's needs, each individual platform may implement the core concepts of blockchain differently (i.e. currency exchange, document sharing, autonomous contracts, consensus transaction or event interpretation, etc.).

Blockchain platforms are ever-evolving. To offer improved performance, some full-featured application development and execution environments are located *off* the blockchain (but are accessible by applications on the blockchain). Others are developed by consortiums in the public domain, offering new opportunities to engage with developers and influence future platform releases.

Programmability

As one of the most important aspects of blockchain is the integration of programmability or decentralized applications (DApps), many platforms are incorporating the concept of distributed applications or computer code. For example, the Ethereum blockchain platform uses "Smart Contracts" to distribute the code along with the blockchain data. It runs on all nodes and, like the data in blocks, has arrived at a consensus on the output of an application. As a security feature, code may include instructions detailing who is permitted to execute the code.

The overall value of this visible programmability is *reduced risk and costs*. Any party can examine the code and verify what will happen if they call or cause the code to execute. Again, the importance to compliance with the DSCSA is that *every single supply chain partner (and regulator) can verify that the code is producing the agreed output given a specific input transaction*. This may alleviate instances where two trading partners interpret transaction information differently, triggering unnecessary exception processes, industry-agreed (consensus) code could reduce the risk to trading partner operations. Additionally, consensus reduces the risk of different interpretations that may trigger unnecessary actions by regulatory inspectors and possibly lower the expense for industry and regulatory agencies.

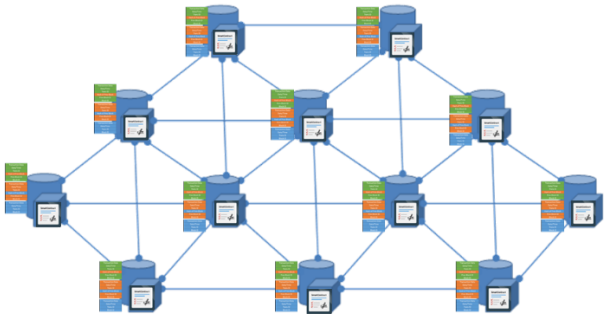

Figure 3 - *Distributed Information and Processing Logic*

Public blockchains

Pure blockchain platform implementations are public blockchains. That is, any person or entity can provide identity credentials on this platform to establish an account. These "public blockchains" provide the most flexibility for individuals, companies and industries seeking to develop shared, distributed applications and data sets without having to maintain the hardware and software used by the applications and blockchain.

The challenge is that all people and companies connected to the platform have visibility to the data and application code, meaning all activities are conducted "in the open" for all to see. Care must be taken to obfuscate sensitive data so that only trusted and permissioned parties can access the data (typically achieved through a combination of data encryption and the use of hash values). Properly designed distributed applications and blockchain datasets can be created so that private persons and companies can openly transact without others able to see the specifics of the transaction. This is all accomplished with native blockchain concepts and data encryption techniques.

Private blockchains

Many platforms allow for the creation of private and permissioned blockchains. In these instances, the underlying platform code is copied to a new location run separately from publicly accessible blockchains. The advantage of private blockchains is that governance bodies or gatekeepers are established to handle the logistics of approving blockchain access. The disadvantage is that because the gatekeeper maintains the underlying code of the platform copy, they are the decision maker on how, when and if any platform changes or updates will be applied. This also may lead to situations we often see with purchased applications where the software owner uses an outdated version that becomes problematic for users.

Performance

Blockchain platforms have been described as big, slow yet *reliable* systems. Those characteristics don't typically bode well for a meaningful discussion on "performance." Remarkable throughput is not a hallmark of current platforms, but help is on the horizon.

Several public blockchains use a "proof-of-work" verification technique to determine what transactions are to be placed in the blockchain. This deters nefarious actors from overwhelming the nodes with transactions intent on shutting down the platform. Essentially, proof-of-work causes a node to solve a difficult calculation, but slows down legitimate transaction throughput. The blockchain community is addressing this issue, creating and testing new protocols as we speak.

There is some new thinking, however, that private (or permissioned) blockchain solutions would not need "proof-of-work" because everyone connected to the platform has already been properly vetted.

Unfortunately, blockchain platforms are not typically known for being able to efficiently store large amounts of data. They also charge a fee for the storage. But this is understandable as all nodes must purchase and maintain the equipment to safely store that data.

Quite a bit of work is being done to enable data storing off the blockchain platform while still making it accessible to distributed applications. One example is the Ethereum platform that has engaged with IPFS (InterPlanetary File System) technology to provide efficient and responsive storage and retrieval of large amounts of data. Other platforms, including BigChain DB, can access IPFS and other solutions that all fit within the timing and the needs of the pharma supply chain relating to the DSCSA.

Funding

Establishing a process for funding a nationwide system to connect each participant in the U.S. pharmaceutical supply chain is daunting at best. A fair method of estimating and establishing fees, along with accounting duties of collecting and disseminating fees, arbitration between disagreeing trading partners and managing access and permission rights to data on the blockchain, all add to the additional overhead needed to operate the system.

Fortunately, most blockchain platforms contain an alternative solution. Many already implement a fee-per-transaction or "calculation" to run distributed applications. These small fees fund the maintenance needed to run the blockchain platform on the nodes and are typically paid using the platform's accepted cryptocurrencies. The payments and distributions are automated, so there is no need for a central body to account for and process collections and payments.

> *A note of interest*:
> As stated above, many platforms assess a fee per calculation to incentivize and reimburse the owner of the node on which the distributed application is run. Because of this, efficient coding practices are directly related to cost reduction for supply chain partners that use those applications. Code sets that require more iterations to accomplish the same task as other code sets is what increases the cost to the user.
>
> The blockchain community is now addressing this issue. *In the meantime*, common code built from industry consensus should be evaluated on processing efficiency, including if it correctly implements the rules.

SUMMARY

Blockchain platforms continue to evolve and incorporate new and extended features that may create new opportunities between and among trading partners. Current platforms are useable for proof-of-concept pilots and other implementations. Development environments and mass data storage capabilities are now being brought together and refined.

Based on identity-credential sharing (proof of licensing, etc.), blockchain platforms provide the capability to connect tens of thousands of supply chain partners. They allow for a sort of "ad-hoc" sharing of information and trade item states that are needed to accommodate complex supply chain processes, mergers, acquisitions and exits from the supply chain. Distributed applications (aka "Smart Contracts") provide the opportunity for the implementation of consensus across supply chain partners and with regulators, reducing risk and expense at every step.

The blockchain community is actively engaged in exploring and implementing features to increase throughput, response time, data storage needs, security and confidentiality. On a transaction basis, the concept of establishing or using a stable cryptocurrency to pay for the upkeep and maintenance of the platform could reduce the cost of otherwise establishing and supporting an overarching body to collect and disperse payments and arbitrate disputes.

RECOMMENDATIONS

Based on our knowledge and understanding of blockchain, we make the following general recommendations:

- Further explore and implement the use of blockchain and the interoperability of its platforms.
- Consider implementing a licensing or certification check when providing access to an industry blockchain solution. The regulators and authorities who issue these certifications already are already considered "the authority" on determining if an individual or company may take a role in the supply chain (manufacturer, 3PL, Wholesaler, Dispenser). These same regulators can also fulfill their role in the blockchain by saving the industry the burden of determining who gets access. It stands to reason that because it is the regulator who grants permission to manufacture, wholesale, transport or dispense certain products, proper vetting has occurred.
- Consider the use of established transaction-based and calculation fees to fund the architecture and distribute payments to those who maintain it.
- Consider establishing consensus-based distributed applications to evaluate posted transactions and help reduce risk.
- Record/document the outcome of the transaction on products and companies using their "states" or "statuses." This will reduce the need for trading partners and gatekeepers to individually determine state/status and further reduce the risk of engaging with nefarious players.

ACTIVITY OF THE CENTER'S DSCSA & BLOCKCHAIN STUDY

In January 2017, the Center initiated a Study on the use of blockchain technology for the purposes of DSCSA compliance. The Team consisted of manufacturers, wholesalers, dispensers (hospitals and retail), reverse logistics providers, 3PLs, providers of track & trace solutions, providers of blockchain solutions, associations, standards bodies, regulators, consultancies and universities. *The Study Team focused on:*

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 system-wide risk

To address DSCSA compliance laws, honor current supply chain practices and allow for individual information-sharing agreements between trading partners, the Study Team established categories of rules for exploration in a simulated environment. Rule categories included:

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

These categories allowed the team to effectively discuss and analyze supply chain scenarios and the impact of blockchain design variations without "blurring the lines" between what is specifically called for in the law, and what may be desired or needed by trading partners.

The team created *ReferenceModels*, or supply chain simulations, to test whether data created in a trading partner to trading partner agreement could be held confidentially in the shared industry blockchain. This clear framework to.

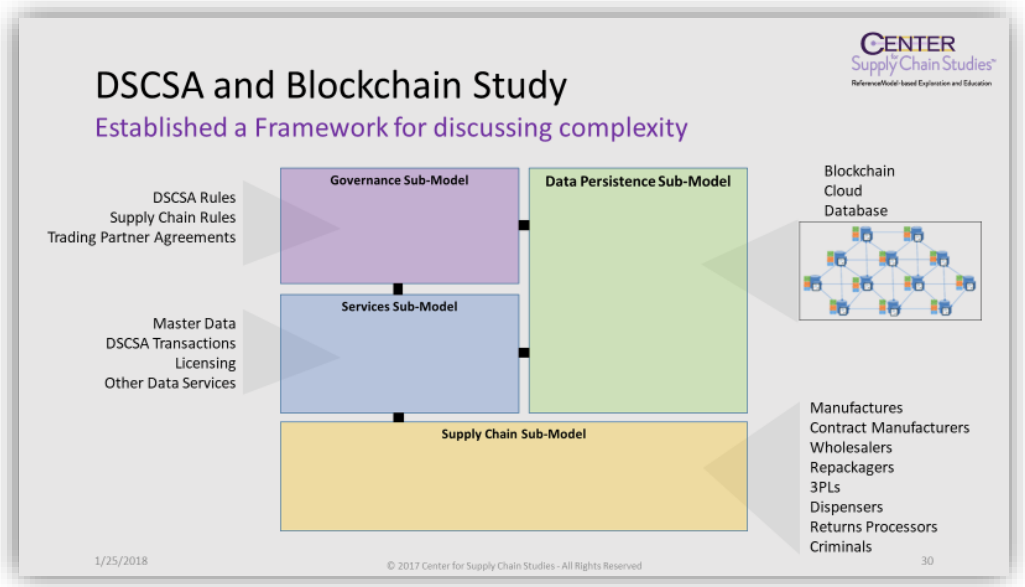

Figure 4 - *Analysis Framework*

In 2018, the Center launched the Study, DSCSA & Blockchain: Phase 2, to execute proof-of-concept pilots from the Phase 1 work detailed above as well as the Blockchain for the Cold Chain Study to explore the use of blockchain to communicate status and underlying temperature data for temperature sensitive products.

FOR MORE INFORMATION

Robert Celeste, Founder
Center for Supply Chain Studies
P:215.584.7374
rceleste@c4scs.org