

2018

Evaluating Feasibility of Blockchain Application for DSCSA Compliance

Tracie Scott

Southern Methodist University, tracies@smu.edu

Armand L. Post

Southern Methodist University, apost@smu.edu

Johnny Quick

Southern Methodist University, jdquick@smu.edu

Sohail Rafiqi

Southern Methodist University, srafiqi@lyle.smu.edu

Follow this and additional works at: <https://scholar.smu.edu/datasciencereview>



Part of the [Operations and Supply Chain Management Commons](#), [Pharmaceutics and Drug Design Commons](#), [Pharmacoeconomics and Pharmaceutical Economics Commons](#), and the [Pharmacy Administration, Policy and Regulation Commons](#)

Recommended Citation

Scott, Tracie; Post, Armand L.; Quick, Johnny; and Rafiqi, Sohail (2018) "Evaluating Feasibility of Blockchain Application for DSCSA Compliance," *SMU Data Science Review*. Vol. 1: No. 2, Article 4. Available at: <https://scholar.smu.edu/datasciencereview/vol1/iss2/4>

This Article is brought to you for free and open access by SMU Scholar. It has been accepted for inclusion in SMU Data Science Review by an authorized administrator of SMU Scholar. For more information, please visit <http://digitalrepository.smu.edu>.

Evaluating Feasibility of Blockchain Application for DSCSA Compliance

Armand Post¹, Johnny Quick¹, Tracie Scott¹, Sohail Rafiqi²

¹ SMU Master of Science in Data Science,

² SMU Adjunct Professor,

{apost, jdquick, tracies}@SMU.edu; srafiqi@lyle.smu.edu

Abstract. We evaluated the feasibility of using a blockchain technology to create a traceability solution for pharmaceutical drugs that would promote compliance with recent legislation. Counterfeit and other illegitimate pharmaceutical drugs threaten patient safety, drug efficacy, and patient trust. The purpose of the Drug Supply Chain Security Act (DSCSA) is to greatly reduce distribution of illegitimate drugs by requiring all pharmaceuticals to be serialized and traceable from the manufacturer through the supply chain to the dispenser. A software application to serialize and track pharmaceuticals must overcome numerous obstacles. In particular, the solution must provide a high degree of trust while also protecting privacy for manufacturers, distributors, and patients. This research will propose that a blockchain-enabled application will solve for many of the most challenging needs for this solution.

1 Introduction

The Drug Quality and Security Act (DQSA); enacted November 2013; set requirements for the compounding safety and security of pharmaceutical products. The law has two focus areas. Title I is “The Compounding Quality Act”, which set standards for safety and security for compounded drugs. Title II of DQSA is the “Drug Supply Chain Security Act” (DSCSA). The DSCSA is further divided into two focus areas. One effort establishes license and registration requirements for all wholesale distributors and third-party logistics (3PL) providers to ensure proper identification of all legitimate members of the supply chain. The second effort requires the consistent traceability of pharmaceutical products from the manufacturer to the dispenser within the United States. Participants in the supply chain are expected to verify the chain of ownership, detect suspicious activity, and respond accordingly as outlined by the law. In addition, participants must be able to quickly respond to requests for information from enforcement officials. The final outcome of Title II will be the creation of an electronic, interoperable traceability system for pharmaceutical products at the package-level by 2023 [1]. The goal is to use real-time data capture to detect, respond to, and report potentially illegitimate drugs faster and more effectively before they can become a safety hazard to patients.¹

¹ AmerisourceBergen. (2017). Serializing Your Products [White Paper].
<https://www.icsconnect.com/insights/serializing-your-products>.

The DSCSA was created to curb the circulation and sale of illegitimate pharmaceutical products. Illegitimate drug products jeopardize consumer safety and cost the pharmaceutical industry almost \$40 billion annually [2]. By serializing the products and providing traceability from manufacturer to dispenser, participants in the supply chain can be protected and have greater assurance of encountering only legitimate pharmaceutical products. However, achieving this goal requires creating a reliable system of record with appropriate visibility to identify legitimate pharmaceuticals for all participants in the supply chain. Since members in the supply chain have compelling business reasons not to share information on inventory, a key challenge to ensuring compliance with traceability requirements will be establishing trust among stakeholders.

Blockchain distributed ledger technology is causing controversy in the industry, with some touting its capability to revolutionize computing while others are not convinced. Gartner lists blockchain as on ‘the peak of inflated expectations’.² In an attempt to clarify the real opportunity for blockchain, SAP surveyed “hundreds of organizations currently engaged in blockchain-related activities”. Of the people surveyed, 92% believe blockchain represented a new opportunity in the marketplace and of those 63% sited supply chain applications as the most promising use cases for the technology.³ Blockchain applications are appropriate when trying to introduce trust into a trust-less system. As such, providing traceability of pharmaceuticals through the supply chain is a suitable use case for a blockchain implementation. This review demonstrates how a blockchain technology can provide functionality that benefits supply chain in general, and traceability of pharmaceuticals in particular.

The case for the feasibility of blockchain for pharmaceutical supply chain is built by first delving into the pharmaceutical supply chain and the DSCSA in sections 2 and 3 respectively. Then we present the characteristics of a blockchain distributed ledger in the context of supply chain applications in section 4. In section 5, we explore how blockchain is currently being implemented in supply chain applications. . The paper concludes with ethical considerations presented in section 6, conclusions in section 7 and a summary in section 8. As this project was originally initiated as a Proof of Concept, efforts to build the POC are outlined in the Appendix.

2 Pharmaceutical Supply Chain

The pharmaceutical supply chain is comprised of excipient manufactures, the manufacturer of the drug, repackagers, wholesalers, logistics partners, and ultimately the dispenser. The FDA provides a simplified illustration of the pharmaceutical supply chain presented below.⁴

² Gartner. https://blogs.gartner.com/smarterwithgartner/files/2017/08/Emerging-Technology-Hype-Cycle-for-2017_Infographic_R6A.jpg

³ SAP. <https://news.sap.com/blockchain-a-study-rooted-in-reality/>

⁴ FDA. A Drug Supply Chain Example. <https://www.fda.gov/downloads/Drugs/DrugSafety/DrugShortages/UCM277651.pdf>.

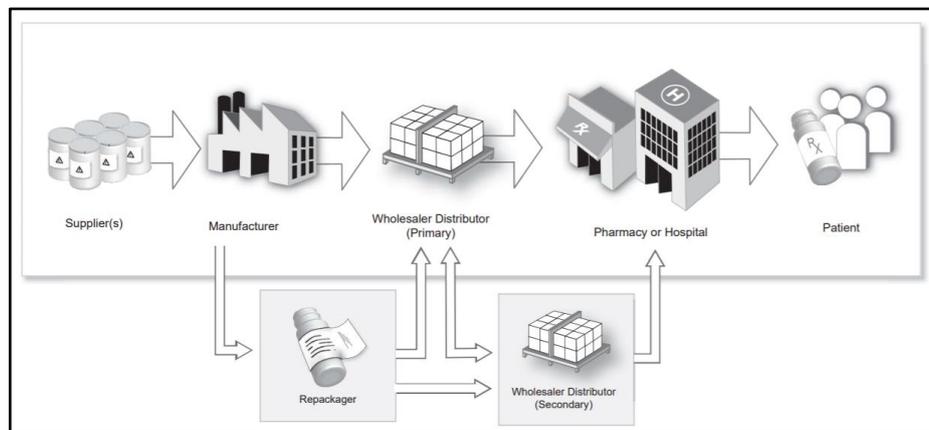


Fig 1. FDA: Simplified View of the Pharmaceutical Supply Chain

Despite the simplified diagram, the pharmaceutical supply chain spans many geographical regions and involves numerous parties. The pharmaceutical supply chain contains excipient manufacturers. Excipients are substances other than the pharmacologically active drug which are included in the manufacturing process or are contained in a finished pharmaceutical product⁵. Only 6 percent of pharma sales are direct from the manufacturer. Various regulations for things such as Medicare/Medicaid compensation and transparency regarding cost revelation from drug wholesalers and manufacturers continually impact the decision-making of pharma supply chain managers and most product flow through a complex web of manufacturers, repackagers, and wholesalers.[3] Repackagers are companies that buy drugs from a manufacturer or a wholesale distributor and then put the drug into a new package type, such as putting the drug into a smaller quantity package or moving units from bottles into a blister card. Transfer of the drug from the manufacturer can be to a repackager, a wholesaler, or directly to a dispenser; such as a hospital, non-specialty pharmacy distributor, or specialty pharmacy. A wholesaler may warehouse the product before selling and transporting to another wholesaler or a dispenser. The end of the pharmaceutical supply chain is the dispensing of the drug to a patient.

The complex nature of the pharmaceutical supply chain includes the fee-for-service model between the wholesaler and manufacturer. Contracts between drug manufacturers and wholesalers help ensure that wholesalers maintain a supply agreed upon by the manufacturer and wholesaler in exchange for a fee paid to the wholesaler by the manufacturer. This arrangement helps the manufacturer to adequately procure raw materials for their drug and to manufacture their drug in accordance with likely demand. Without this contract in place, wholesalers may buy in excess to hedge against price increases which would artificially inflate demand [4].

⁵ Rutesh, H. Dave, (2008). *Overview of pharmaceutical excipients used in tablets and capsules.*

GlobalData predicts that the estimated value of the US Pharmaceutical market will increase from just under \$400 billion in 2014 to almost \$550 Billion by 2020 [5]. The complexity of the supply chain increases as new drugs and new types of drugs are developed, more functions are outsourced globally, modern technology is introduced, and new regulations are enacted. Considering the increasing complexity of the supply chain and the enormous monetary value at stake, it's not surprising that securing the pharmaceutical supply chain both urgent and challenging.

2.1 Risks in Pharmaceutical Supply Chain

The top three risks to the supply chain are 1) theft or diversion, 2) introduction of counterfeit medicines, and 3) contamination of medicines during manufacturing, storage, or distribution [5]. A diverted product has been removed from the normal United States supply chain and then reintroduced for sale. This may include a drug labeled for sale outside the US but then introduced into the US market, or a drug transported outside of the US but then reintroduced within the US supply chain [6]. Provenance and authenticity are hard to verify for diverted drugs, raising questions about safety and effectiveness. According to the FDA, a counterfeit drug is one in which the container or labeling falsely represents a stakeholder in the supply chain, such as the manufacturer, processor, packer, or distributor of the drug. A counterfeit drug is sold with the intent to defraud and represents numerous risks to the consumer. Examples include products that contain none of the active ingredient, an inappropriate dosage of the active ingredient, or ingredients not on the label. The product may have ingredients not in the original, meaning the specific combination has not been tested or approved by the FDA. In 2008, a counterfeit version of the blood thinner heparin may have contributed to the deaths of 81 people in the United States [5].

Typically, the objective of a supply chain is to maximize overall value created. Supply chain management often focuses on cost reductions and efficiencies to achieve that goal [7]. Considering the many avenues for fraud with potentially significant adverse consequences for the patient, pharmaceutical supply chain management must prioritize safety for the end user. Often, added safety measures and cost controls are opposing goals. The DSCSA is first seeking to assure the safety of the pharmaceutical supply chain by decreasing and detecting incidents representing the top risks of theft, diversion and counterfeiting, but in doing so may also protect supply chain participants from significant financial loss as well.

2.2 Lack of Integration across Pharmaceutical Supply Chain

As complex as the physical supply chain is, the information flow, document exchange, and payment processes are even more complex. Think of each organization in the chain as having its own inventory/receiving/payables/accounting systems behind their firewall. These systems represent a myriad of different platforms, protocols, database, and data models, each operating independently within each participant with no inherent trust across the supply chain. In fact, within one supplier, systems may be operating with limited integration. Even as operations move to the cloud, the systems are still

independently owned and operated, with each entity owning their data if not the applications and infrastructure. Connecting this collaboration of buyers and sellers is an array of third-party data transfer services that ‘map’ the buyer’s data to the seller’s data to facilitate electronic transfers of orders and other information. Electronic Data Interchange (EDI), Hub models and cloud integration solutions provide some connectivity, but there is no common data model used end-to-end across the supply chain [8]. Plus, even with electronic transfer and data interchange, some level of manual intervention frequently remains. For example, a person may need to enter the order, and someone on the dock has to receive the shipment and verify the count and contents. These activities may require manual data entry that introduces an opportunity for human error.

Along with other perishable products, pharmaceutical products are increasingly monitored for temperature and other environmental conditions during shipping and storage. Drugs can be rendered ineffective if exposed to adverse environmental conditions. Leveraging RFID technology and the connectedness of the Internet of Things (IoT), more companies are piloting programs to embed sensors within product shipments then monitor and analyze the resulting data to be sure the quality of the product was not compromised as well as to be able to track and locate containers in a shipment [9]. While obviously providing value and increasing safety, this also creates more complexity as that data must be received, analyzed, and used as part of the contractual agreement.

Furthermore, each participant may have a financial partner, such as a bank, performing trade finance functions on their behalf. For example, the seller’s bank will guarantee that the seller can supply the product and has delivered what was agreed. The buyer’s bank guarantees that the buyer has received what was delivered and is able to pay. Banks may provide letters of credit, document collection, buyer/seller credit, bank guarantees, trades insurance, and other trade finance services to participants in the supply chain. The need for trusted intermediaries effectively doubles the participants in the transaction and drives complexity [8].

Theoretically, if the parties were sharing a blockchain, these trade services could be eliminated, but that is outside the scope of what is required by the DSCSA, but the requirement to provide traceability of drugs is a core requirement within the information flow of the pharmaceutical supply chain. If there were an end-to-end data exchange standard already defined for the pharmaceutical supply chain, then perhaps implementing DSCSA would not be as large a challenge.

3 Drug Supply Chain Security Act (DSCSA)

The DSCSA stipulates the drugs and drug transactions that are covered by the act. The DSCSA applies to all prescription drugs in “finished dosage form for administration to a patient without further manufacturing” [1]. Excipient manufactures are excluded from provisions. The DSCSA does not apply to blood or blood components intended for transfusion, radioactive drugs or biologics, imaging drugs, certain IV products, medical gas, homeopathic drugs, and lawfully compounded drugs. The DSCSA applies to all transactions where a change of ownership occurs unless specifically exempted.

Exemptions include intracompany distributions, distributions among hospitals under common control, public health emergencies, dispensing pursuant to a prescription, and transfer of approved animal drugs [1].

The primary activity being regulated is the transfer of ownership of the pharmaceutical. With each change in ownership, “product tracing information” should be exchanged and consists of three types of information:

Transaction Information (TI). The TI includes name of the product, the strength and dosage form, the National Drug Code (NDC) number, the container size for individual saleable units, the lot number, the date of the transaction, the date of shipment, and the business name and address from whom and to whom ownership is being transferred.[1] The NDC is a three-segment number comprised of the labeler code, the product code, and the package code. The FDA publishes the NDC numbers for finished drugs in the NDC Directory, which is updated daily. Future requirements may also include the number of containers, meaning the number of individually saleable units within the lot [10].

Transaction History (TH). The TH details the transaction information above for each prior transaction going back to the manufacturer of the product. This information establishes the chain of ownership that validates the pharmaceutical is legitimate.[1]

Transaction Statement (TS). The TS establishes accountability under the law for the entity transferring ownership. The entity transferring ownership attests that they: are properly authorized under DSCSA, received the product from an entity authorized under DSCSA, received TI and TS from the prior owner as required under the law, did not knowingly ship a suspect product, have systems and processes in place to comply with verification requirements, did not knowingly provide false transaction information, and did not knowingly alter the transaction history [1].

Any entity who takes ownership of a covered drug from the manufacture of the final form through the dispenser is impacted by the act. Repackagers have most of the same requirements that manufacturers do, plus they have many of the wholesale distributor requirements. Under DSCSA, entities that own the drug may also be “repackagers”, such as a hospital that repackages bulk medication into individual units used with automatic dispensers.

3.1 Validation Requirements

A drug is considered a suspect product if there is reason to believe it was potentially counterfeited, diverted, stolen, part of a fraudulent transaction, intentionally adulterated or is otherwise unfit to distribute for patient safety reasons. An illegitimate product is any drug with credible evidence that the product is any of the above.[6] Note that the designation does not require proof. With this act, the FDA effectively shifts responsibility onto the seller via the TS not just to verify legitimacy of the product, but to report and investigate suspected violations. Verification requires establishing systems and processes to comply with verification requirements, including the ability to: respond to verification requests from the FDA about suspect products, quarantine and investigate suspect product, notify trading partners and the FDA of illegitimate product within 24 hours of determination, respond to notification of illegitimate product, and maintain records.[1] Drug dispensers must be able to comply with requests

for information, providing TI, TH, and TS, within two business days while other stakeholders in the supply chain must respond one business day [1].

3.2 Timeline Requirements

The first milestone of the act allowed the product traceability information to be provided in either paper or electronic form. Future milestones include dates when the stakeholders in the supply chain must convert from paper to electronic forms. Other key dates for the act include when stakeholders must only buy and sell products encoded with product identifiers (aka serialized products) as well as when verification must switch from lot-level to package-level identifiers.



Fig. 3. Current Timeline of DSCSA

While some tenants of the act have already been postponed or relaxed, manufacturers are under pressure to create systems and processes for traceability to be compliant with the law. However, achieving this goal requires creating a reliable system of record with appropriate visibility for manufacturers, repackagers, wholesale distributors, and dispensers.

4 What is Blockchain?

Blockchain is a distributed ledger software technology, meaning it's a peer-to-peer (P2P) public ledger maintained over a network of computers.⁶ Blockchain provides a method for storing information in a distributed fashion without relying on a centralized database maintained by a trusted party. The name reveals its method. Transactions are clustered into blocks of data that are fit together chronologically into a chain using a hashing algorithm that theoretically makes the confirmed records immutable. The blockchain is replicated to each participating node on the network and administration of the blockchain software is orchestrated by consensus of the participating nodes.

The term "blockchain" appears to have originated from a reference to a "chain of blocks" by Satoshi Nakamoto (pseudonym) in 2008 as a method of validating

⁶ Scott, Post, Quick "The Best Thing since the Internet: Blockchain" SMU MSDS term paper.

ownership of virtual currency in a publicly distributed ledger. Nakamoto's purpose for suggesting a peer-to-peer electronic cash system was to make powerful, centralized third parties obsolete by disintermediating financial transactions.[11] In 2009, the first application of blockchain technology appeared in the source code for the digital cryptocurrency Bitcoin. The Bitcoin blockchain is a public ledger of all the Bitcoin transactions that have ever taken place.

Exposing a transaction's footprint to the marketplace is called 'leakage' and leads to a host of undesired market behaviors. Preventing leakage is one reason why transaction data is protected in corporate databases. If the blockchain data is public, then what prevents competitors from clearly seeing all the transactions? How can a technology bind the identity for shared data yet provide anonymity at the same time? Blockchain uses encoding technologies to provide privacy, including hashing algorithms and public key cryptography.

The heart of a blockchain is a hashing algorithm⁷. A hashing algorithm is used to map data of varying lengths to an output of fixed length. The values returned by a hash algorithm are called "hash values", "hash codes", "digests", or simply "hashes". Any change to the original data would result in a different hash output. Changing a space or a letter or even changing a lowercase letter to an uppercase letter in the data would cause the output hash value to be different. Since the input hashes to a unique value, and it's infeasible to produce a different block that hashes to the same value, the digest provides assurance that the original data has not been altered. The Bitcoin Blockchain relies on SHA-256 to create a 256-byte block that represents the input data. These are the 'blocks' in a blockchain.

In addition to using hashed encoding, blockchain also uses private key cryptography. Public key cryptography is an encryption system that uses pairs of keys to encrypt and decrypt data. On the blockchain, each entity is assigned a "public key" available to all participants and a "private key" that is provided only to the entity it identifies. The keys are used for authentication. A message or document can be encrypted with a private key. If the message is legible when it is decrypted using the corresponding public key, it's guaranteed that the holder of the private key is the party that encrypted the message. This digital signature serves as an encrypted, unique identifier associated with a registered member of the blockchain. Blockchain also supports a concept called M-of-N signatures or "multisig," meaning that there exists a total of N cryptographic keys, and at least M of them have to be present to decrypt the data.[12] Since each transaction includes the digital signature, the parties to the transaction are known. Because it's an encrypted key, the real-world identity of the parties can be protected.

As you would expect, the ledger records transactions, like "Billy sends Sally 10 Bitcoins", but other pieces of data are required in the block as inputs to the hashing algorithm. Each transaction contains the digital signature of the sender and a timestamp. The hash value for the previous block is included as input for the current block. This inclusion forms the 'chain', with each new block being linked to the prior block. The input also includes a nonce, or "number used once", which is a random numeric value that creates a hash that will be accepted by the blockchain. Other values are included as well, but these are the basic components of the input string. Once the inputs are assembled, the input string is hashed to create a 256-byte value. If the resulting value

⁷ Scott, "Blockchain" SMU MSDS term paper.

is accepted by the network, the block is added to the chain and validated by other members. The block is added to all the distributed nodes, and the process continues for the next block.

In a proof-of-work implementation like Bitcoin, miners supply computing resources and receive compensation for adding valid blocks to the chain as well as transaction fees for each transaction in the block. Miners race to find a nonce value that will create an acceptable hash value from the data inputs. The network sets an adjustable threshold to regulate the difficulty and thus the length of time, for solving the puzzle of discovering a nonce to complete the block. This mechanism keeps a pace of one new block added to the chain every 10 minutes. As new blocks are added, they are considered 'confirmation' for the prior blocks. Once six confirmations have been added on top of a block, the data is considered immutable. At that stage, it's not feasible with today's computers to alter the input data for a block, find a new nonce, add a block with altered information, and then somehow race ahead to beat all the other computing resources on the network to rebuild an alternate chain.

While this is a greatly simplified description, it provides a basic framework for understanding the blockchain technology. Since its introduction, Bitcoin blockchain has expanded functionality and now allows more types of transactions to be programmed into the blockchain. After ten years of effective use with Bitcoin, blockchain technology is now being considered as an alternative to centralized accounting ledgers and other track-and-trace record keeping systems. Plus, since it's the forerunner of all other blockchain solutions, it's important to understand the characteristic strengths and weaknesses of the technology.

4.1 Key Characteristics of Bitcoin Blockchain

Let's take a closer look at the traits that, collectively, position the Bitcoin blockchain to provide a unique and compelling solution to the marketplace.

Data Structure. Transactions are formatted into blocks that are linked together using a cryptographic hashing algorithm that takes as input data from prior entries such that the output is a secure chain of data in which one block cannot be altered without invalidating the hash.

Distributed. Every node in the network contains a full copy of the dataset.

Decentralized. An algorithm is used by the nodes to validate new entries, with entries that are validated by a majority of nodes included in the blockchain. Not only are transactions verified by consensus, but updates to the blockchain software are also accepted by consensus.

Transparency with Privacy. Users have a digital signature, and each transaction includes the digital signature of the parties involved, but the signature is not easily associated with an individual or organization.

Timestamps. Timestamping assures the order of transactions is accurate. Combining these traits creates a secure, publicly-sharable database that reliably records the time, content, and parties of each transaction without centralized control for data or software updates. Compare that to privately-held, centrally managed databases that are susceptible to alteration of individual data components. To simplify, traditional technology says "I have my data. You have your data. We have to validate and reconcile

activity between our databases using a bank or a trusted third party to facilitate. As soon as the reconciliation concludes, either of us can change our data such that I no longer trust who you are or your data.” Blockchain technology has the potential to say “I know who you are. I know who owns this asset. We have a shared record of trusted, validated transactions; no reconciliation required.”

As a result of these traits, blockchain offers several key benefits compared to traditional approaches.

Data Integrity. The cryptographic, secure nature of the data structure removes questions about asset identity, asset ownership, and transaction history. Hashed blocks make it unfeasible to reverse or tamper with transactions.

Operational Resilience. Distributed data model means data is always accurate and accessible.

Built-in Audit Trail. Time and parties to transactions are built into the data structure itself, automatically establishing audit trails while protecting privacy since parties are identified only by public/private keys.

Ownership. Provides an immutable record of ownership and effectively prevents double-spending of assets.

The potential to create a secure, shared, immutable record of transactions and asset ownership is predicted to drive the mass adoption of blockchain technologies as the next logical step in application evolution. Blockchain instantiates trust as part of the application.

4.2 Challenges of Bitcoin Blockchain

While the promise of blockchain is great, the associated barriers and risks are also great. Some of the commonly cited challenges to the adoption of blockchain are listed below.

Blockchain Applications not Impervious. The blockchain is a data store. As with any other data store, an application is written to leverage the functionality provided by the data store. Even if the data store is secure, the application may provide vulnerabilities. Exchanges have been hacked on multiple occasions since they store both public keys and private keys. Hackers can quickly drain wallets if they are able to break in and obtain the keys. The underlying assumptions of the benefits of blockchain have been challenged by two well-publicized events. First, a cyber attack on Ethereum, a smart contracts blockchain application, improperly diverted \$50M worth of tokens. To counter this attack, 85% of Ethereum users voted for a ‘hard fork’ of the chain, which essentially rolled back the effects of the attack and restarted the chain before the attack. The remaining 15% of users continued to use the affected data, referring to it as ‘Ethereum Classic’. The second event involved the bankruptcy of Mt. Gox, who held 70% of Bitcoin traffic in 2014. During the course of the bankruptcy, it was discovered that \$450 million in Bitcoin was stolen from the bank.[13] These two events shook confidence in the blockchain software as vulnerabilities became apparent.

Technical Limitations. Scalability is a critical concern as no cryptocurrency platform approaches processing the number of transactions with the speed of large payment systems like VISA.[14] Capacity, latency, and query capabilities are quite limited in comparison to other distributed database systems.[13] Currently, there are no protocols or standards for interoperability with blockchain. Even with the cryptographic

nature of blockchain, the breaches and vulnerabilities discussed earlier point toward remaining security challenges. Plus, with such a widely distributed architecture, there are simply more entry points for cyber-attacks to occur using methods unforeseen at this time.

Government Regulation. Healthcare and pharmaceuticals are heavily regulated, so any change in technology would need to be proven to comply with regulations. There has been no uniform regulation of cryptocurrencies globally let alone addressing the implications of a blockchain's recording transactions for non-monetary assets. Plus, regulation can create a culture that does not quickly adopt change. "Years of heavy regulation and a long-standing focus on compliance have co-opted the ability of the healthcare industry to implement novel data sharing approaches. We now face a critical need for such innovation. The primary challenge to adoption of blockchain technology in healthcare is that it is still a nascent technology".[12] Looking specifically at the US stock market system, much of the infrastructure has developed 'organically' over decades to meet needs of users and regulators. Switching to a whole new architecture would be risky, so rapid change of the infrastructure is unlikely.

Conflicting International Law. The General Data Protection Regulation (GDPR) prevents misuse of personal information collected in databases for citizens of the European Union. The law was passed April 2016 but goes into effect May 2018. One tenant of this law is that people have the right to ask for their personal information to be removed from databases once the need for the data is complete. This requirement is in conflict with the architecture of blockchain. Because blockchain data is immutable, by definition the data can't be removed. However, SQL databases, data changes are actually logged over time, so the probability that personal data is actually 100% deleted is not likely. The most likely implementation is that data should not be viewable, usable, or sharable. This could be accomplished by not putting personal data into the blockchain. Personal data could be kept in a different data store with a link to the external data being in the hashed blockchain. Given that decentralized blockchain applications have no way to remove prior data and no centralized authority to request removal from, it is essentially the responsibility of the person conducting transactions and putting data into the chain not to share personal information or not use the service. Other laws in the EU regulate where data can be stored, with some data not allowed outside country borders. Because the blockchain is usually replicated to all nodes, any global blockchain implementation is going to contain data from all participating countries in all nodes.

While there has been no coordinated global regulation for cryptocurrencies or blockchain, many countries have begun regulation of their own. Most of the regulation revolves around what type of asset class cryptocurrencies should be considered, whether or not exchanges are legal, and enforcement of money laundering and "know your customer" laws. In addition, there is no consensus on what type of asset class cryptocurrencies should be considered, even within individual countries. In the United States, the SEC considers cryptocurrencies as securities, the Commodity Futures Trading Commission considers them a commodity, while the IRS considers them as

property.⁸ Below is a summary of various governments' current views on exchanges and Bitcoin's use as legal tender.

Table 1. April 2018 Cryptocurrency and Exchange Status by Country

Government	Exchanges	Legal Tender
Japan	Legal, if registered with the Japanese Financial Services Agency.	Yes
USA	Legal, depending on the state. Must be registered with the SEC.	No
European Union	Legal, depending on the country.	No
United Kingdom	Legal and need to register with the Financial Conduct Authority.	No
South Korea	Legal, if registered with South Korea's Financial Services Commission.	No
China	Illegal	No
Singapore	Legal, may fall under regulatory purview of the Monetary Authority of Singapore.	No
India	Legal. The Indian government has issued warnings but does not currently regulate exchanges.	No
Switzerland	Legal, need to register with the Swiss Financial Market Supervisory Authority.	Yes

Technocrats. While blockchain may move a process away from central authorities of banks and government regulation, it may draw its users toward the power of a technical oligarchy. He who controls processing power may control the blockchain. Changes to the Bitcoin blockchain software occur via a passive process when holders representing more than 50% of the network's mining power adopt or reject a change. Since consensus decisions are based on mining power, there is a potential for the most powerful miners to accept only the code changes advantageous to themselves, shoring up their power. Other situations involving coercion or collusion are also conceivable. Lessor miners could receive compensation (aka bribes) for accepting code changes of little importance to themselves. Software changes could be packaged to deceive those accepting them. Advantageous changes may go unnoticed. This decentralization of authority over blockchain might leave it vulnerable to sabotage. Theoretically, a saboteur could compromise the integrity of the blockchain data either by having a much faster supercomputer than anyone else or by adding enough CPU power to the network

⁸ Rooney, K. (2018). *Your guide to cryptocurrency regulations around the world and where they are headed.* <https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html>

to control a majority of the mining power and organize a so-called “51% attack”. Thus, there is concern that this concentrates too much power and decision making in the hands of technologists, like developers and system administrators. If the system is coded and managed by a select group of technologists, it could be modified to their advantage or to the disadvantage of others.

4.3 Addressing limitation of Bitcoin Blockchain

New products and implementation options offer alternatives to the Bitcoin blockchain implementation to mitigate the challenges listed above. While the term ‘blockchain’ and ‘the blockchain’ are frequently used to refer specifically to the Bitcoin blockchain, a host of alternative solutions and complementary products have been introduced. Increasingly, the terms ‘shared ledger’ and ‘distributed ledger technology’ (DLT) as well ‘blockchain’ are used to generically refer to blockchain solutions. To be a ‘blockchain’, most of the core benefits of the original must be preserved. Obviously, it must provide a decentralized ledger that provides trusted (immutable) provenance, transfer, and tracking of asset ownership. A common theme of most, if not all implementations, is the use of public key infrastructure to secure the asset and hashing routines to link and protect data integrity.

Alternative implementations feature changes to application scale, the “wallet” asset, and the access paradigm. Mining is one of the core aspects of the Bitcoin implementation and was developed to both prevent the fraudulent creation of blocks and to entice dedication of computing resources to the blockchain. Miners receive transaction fees and tokens for creating blocks on the chain. Mining is one of the more controversial aspects of the bitcoin implementation and is modified in or excluded from alternatives. The processing power required to mine is considered ‘proof of work’. While proof of work plays a key role in securing the immutable nature of the chain, it also represents a tremendous amount of wasted computing power. Alternate implementations have moved to different methods, such as ‘proof of stake’ to provide a similar functionality while conserving the processing power and thereby increasing scale and throughput. The Bitcoin blockchain is used to record transactions for a cryptocurrency, but the “wallet” asset can be any physical or digital asset, such as a property title, a birth certificate, patient medical records, or ownership of a serialized drug. Lastly, while the Bitcoin blockchain is a public ledger, a permissioned, private blockchain implementation may be better for building a pharmaceutical supply chain ledger. Also, Bitcoin blockchain is purely decentralized. As aspects of software maintenance are governed by consensus and there no central authority. If you lose your private key, you lose your bitcoin. There is no authority to which you can appeal but there is also no central authority to be intimidated by a government. Some of the alternate implementations, such as what we are proposing for the pharmaceutical supply chain, require a bit of centralization and control to achieve the goals of the implementation. Miners are not collecting fees to supply resources, so participants are likely to supply computing resources and/or pay membership fees to participate.

In addition, there are technologies emerging that are complementary to blockchain that greatly enhance the impact of the technology. One of the key technologies is ‘smart contracts’, which is a key feature of Ethereum. Smart contracts are not traditional legal

contracts. They are blocks of code that ‘autonomously’ execute transactions on the blockchain if conditions in the code are met. The power and promise of blockchain for supply chain application tends to lie the combination of three technologies: 1) using sensors embedded with the product as part of the IoT to record provenance and track location as well as a host of environmental factors, 2) using smart contracts to execute transactions when agreed upon conditions are met and 3) using blockchain to create an immutable record of it all, including current ownership of the asset. In this scenario, it seems reasonable that technology could remove enough risk to reduce the need for intermediation. “Blockchain-enabled smart contracts bring more certainty and reliability to online transactions than has been available to e-commerce environments for the past twenty years.” [16]. Smart contracts can deliver significant benefits to the way that we manage supply chains and regulate variable payments.

5 Blockchain and Supply Chain Industry

A range of uses for blockchain have been proposed for the healthcare and pharmaceutical industries. In 2016 Aptea and Petrovskyb proposed using blockchain to track the supply chain for excipient pharmaceuticals.[17] As of 2018, a wide assortment of blockchain programs are underway. We will highlight a selection of the pilot program implementations mentioned in scholarly works concerning the use of blockchain in the supply chain, paying special attention to those applications that provide provenance and traceability of products since those functions are key to DSCSA compliance. We started by reviewing applications supporting an array of industries within the supply chain and then moved to those applications supporting the pharmaceutical supply chain. We then assessed blockchain applications expressing support for the DSCSA.

Provenance. Provenance conducted a pilot project in Indonesia to enable traceability in the fishing industry.[18] By using mobile phones, blockchain technology, and smart tagging, Provenance tracked fish caught by fishermen. The pilot successfully tracked fish in Indonesia for the first six months of 2016. In July 2016, Provenance started to work with the UK’s retailer Co-op in order to track fresh food such as fish, eggs, and dairy through its supply chain. Co-op customers are able to access information on the product journey through an app on their smartphones. Through deploying blockchain technology while collaborating with external certifiers and auditors, Provenance meets the increasing interest of customers to have reliable information about the source, safety, and sustainability of their products.

Everledger. Working in partnership with Barclays, London-based startup Everledger offers a blockchain-enabled traceability application providing a fraud detection system for luxury items such as diamonds, art, and wine. The verification of the asset is recorded on the blockchain, and insurance companies, owners, and law enforcement can easily check if an asset has been registered. The main goal is to offer digital certificates to prevent insurance fraud as it’s estimated that almost 70% of fraudulent insurance claims are undetected. However, similar to Provenance, the ledger also offers reassurance about product source, in this case, that diamonds are ethically-sourced from “conflict free” regions amid concerns rebel movements use diamonds to

finance wars against legitimate governments.[20] Everledger's diamond registration application runs on a private Ethereum blockchain, provided by Eris Industries. [18,19] While Everledger's diamond industry applications use a certificate system to authenticate diamonds, for wine Everledger attaches a tamper-evident RFID tag on the bottle's cork. Maureen Downey's company Chai Consulting and Everledger developed the Chai Wine Vault⁹ to protect high-end wines. The IBM-based ledger gives each bottle a unique digital identifier, including over 90 pieces of descriptive data related to ownership and storage history. The digital data is updated with ownership changes and storage records and can be used to verify provenance by retailers, warehouses, and auction houses. [20]

Maersk. The Danish shipping company Maersk has successfully tested the use of blockchain applications in international logistics. They started by studying logistics requirements. In 2014, Maersk tracked a shipment of perishable goods from East Africa to Europe and discovered the shipment required stamps and approvals from up to 30 people, including over 200 different interactions and communications. Afterward, Maersk partnered with IBM to start working on a version of its blockchain application based on the Linux Foundation's open source Hyperledger Fabric. IBM and Maersk conducted a successful proof of concept from September 2016 through February 2017, tracking three transcontinental shipments of perishable goods. A successful pilot project was completed in February 2017 that tracked an empty container from a customer site in France through its global transportation to the container's destination in the US.[20] The project is expected to go into production by the end of 2017.¹⁰

Walmart. On May 31, 2017, Walmart released the results of the food safety and traceability protocols test that started in October 2016. The first project involved tracking produce from Latin America to the United States. The second involved moving pork products from Chinese farms to Chinese stores. Walmart partnered with IBM to develop the service. Walmart reported that blockchain helped to reduce the time to track food from days to minutes.[20]

Bext360. Denver-based startup Bext360's app and cloud-based software employ Stellar blockchain to record timestamps and value of transactions on a real-time basis. It creates records of the origination of coffee beans as well as the price paid for the beans. Bext360's first venture will be a kiosk, where farmers can sell beans. A mobile robot allows coffee buyers to assess the quality and weight of a farmer's product in the field while a mobile app supports the negotiation of a fair price. The farmers are paid in real-time via a mobile app.[20]

Intel. In April 2017, Intel revealed a public demonstration that explains how a seafood supply chain can be tracked using its open-source Sawtooth Lake codebase.¹¹ Data for four transactions from October 2016 was made public. The data included the record where a fisherman registered the fish upon catch and then sold it to a fishmonger, IoT telemetry and temperature data associated with the journey from the ocean to the fishmonger's store, the fishmonger's record of selling to a seafood restaurant, and IoT telemetry and temperature data associated with the journey from the fishmonger to the seafood restaurant.[20]

⁹ Winefraud.com. <https://www.winefraud.com/chai-wine-vault/>.

¹⁰ cointelegraph.com, 2017

¹¹ <https://01.org/sawtooth/>

Clearly, these efforts demonstrate emerging capabilities achieved through the application of blockchain technology, especially when coupled with IoT and smart contract capabilities. Most of these trials are expecting to move beyond initial experimentation. However, as encouraging as these successful trials are, none are operating at a scale expected of a global enterprise application.

5.1 Blockchain and Pharmaceutical Supply Chain

We will now consider some proposals, trails, and implementations that are within the pharmaceutical supply chain. Shireesh Apte and Nikolai Petrovskyb proposed the use of blockchain technology to establish provenance and track the excipient supply chain. Recall that excipients are components of drugs that are not the active ingredient. Tracking excipients is not part of DSCSA and there is far less risk of theft, diversion, or counterfeiting of them. But even so, much like people what to know where their fish comes from, using blockchain to track these components assures the safety and quality of the entire pharmaceutical supply chain. Of interest in the article was the insight that blockchain does not alleviate the need for a physical quality audit as data collected from sensors embedded in a shipment cannot fully guarantee the contents were not stolen, altered, or replaced with counterfeit goods [18].

Nuco. The blockchain company Nuco attempts to address three common tactics used in prescription drug fraud: modifying quantities to change the prescription itself, duplication of prescriptions and visits to many doctors to collect multiple original prescriptions. When a prescription is produced by a doctor, a machine-readable code is attached that serves as a unique identifier. This unique identifier is then associated with the name of the drug, the quantity, the patient, and a timestamp and then recorded on the blockchain. When the prescription is filled by a pharmacist, the symbol is scanned, the attempt to fulfill the prescription is compared against the blockchain, and the pharmacist is quickly informed whether the prescription is eligible to be filled. HealthChainRx and Scalamed are also working on blockchain solutions to combat prescription fraud. Several other healthcare-related blockchain applications are in initial stages, including Medicalchain, Healthcoin, BurstIQ, Factom, GemOS, HealthCombix, MedRec, Patientory, SimplyVital, and Bowhead. While these applications were related more to the patient experience or medical records than to supply chain, it's telling to have so many projects initiated addressing different aspects of the healthcare experience [21].

Modum. A recent regulatory change in the EU, known as Good Distribution Practice of Medicinal Products for Human Use¹² requires companies to report any deviations in temperature or other conditions to the distributor as well as the recipient of the affected medicinal products. As a result, pharmaceutical drugs are being transported using expensive refrigerated trucks to maintain conditions that avoided notification, even if the drug did not need refrigeration to maintain potency [21]. Modum.io AG, a Swiss start-up, partnered with the University of Zurich to design a system to ensure the safe transportation of pharmaceutical drugs without the unnecessary use of refrigerated trucks by focusing on the products that can be stored at ambient temperatures (15° – 25 °C). Modum built a prototype and completed a first pilot project together with

¹² GDP 2013/C 343/01

pharmaceutical distributors. From July 7th to August 12th 2016, a pilot project was conducted and medical goods were shipped weekly from one supplier to a pharmaceutical wholesaler. A Modem sensor monitors the temperatures of the medicines during transport and the data is transferred to the Ethereum blockchain after the trip. A Solidity-based smart contract compares the data against regulatory requirements, and if all the required conditions are fulfilled, the product is released. These results are publicly accessible and reported back to the receiver as well as to the distributor. Currently, modum.io AG is planning for a second pilot project with over 500 shipments with more distributors and wholesalers. Must like DSCSA, the Falsified Medicines Directive (FMD)¹³ requires individual pharmaceutical packages to have a serial number to support tracking of medications at ‘per use’ level by 2019. Once packages are serialized, results may also be available to end customers [21].

Gemalto. Gemalto has teamed up with an insurance company that covers the delivery of temperature-sensitive medicines from drug manufacturer to hospitals located in hot climates. Digital thermometers are used to record the temperature of drugs regularly and the data is added to a blockchain ledger. Blockchain helps to govern that process and provide assurance that safety requirements are met [21].

Blockverify. Blockverify is a US company trying to introduce Blockchain into the global pharmaceutical supply chain to avoid counterfeit and forgeries. [20] Their main business areas include pharmaceuticals, luxury items, diamonds, and electronics. Blockverify conducted a pilot project in the pharmaceutical sector using the Bitcoin blockchain together with a private side chain. Every product has its private key stored in the public blockchain that can be verified by anyone. With a track and trace number, it is possible to trace change of ownership, thus every change will be recorded in the private blockchain [21].

5.2 Blockchain application targeting DSCSA compliance

Chronicled, a San Francisco-based blockchain startup, in conjunction with LinkLab, a life sciences supply chain consultancy, launched Mediledger, a blockchain-based compliance protocol to satisfy DSCSA.[20] Like others, Chronicled is not limited to pharmaceuticals and is expanding their service to luxury items. Their blockchain is an open registry where information about buyers and sellers are stored. Luxury items are tagged for identification which allows everyone to check the history of buyers and sellers [21].

Mediledger provides provenance and traceability of drug shipments, supply chain integrity, and real-time global supply feedback using IoT. MediLedger’s stated purpose is to demonstrate compliance with the DSCSA and to create an operable system in which multiple parties can verify and transfer pharmaceutical products with absolute trust in their authenticity, based on blockchain technology. In March 2018, MediLedger released a year-end report in which they stated, “First, the Project’s blockchain-based system appears to fully meet the requirements set forth by DSCSA and is capable of acting as the interoperable system for the pharmaceutical supply chain prescribed in the Act. In addition, MediLedger has proven that it can meet the data privacy requirements

¹³ EU 2016/161

of the pharmaceutical industry itself. In particular, it can guarantee that all supply chain handshake transactions posted to the blockchain are fully obfuscated, ensuring that no business intelligence is leaked. This will allow nodes in the blockchain system to be hosted by numerous unique parties while both safeguarding sensitive transactions and ensuring the immutability of each supply chain handshake transaction.”

5.3 Encouraging Participation

So far, the literature has assumed that pharmaceutical companies will comply with the law, regardless of the cost, because of the governance power of the FDA. However, can the FDA afford to punish all drug manufacturers and other supply chain participants if there is a widespread inability or unwillingness to comply? Perhaps more “carrot” and less “stick” will help encourage participation. Below are some ideas to incent pharmaceutical companies to collaborate in the building of a shared ledger.

Expedite the approval process. This would reduce time to market for new drugs and give manufacturers quicker access to revenue that would help cover R & D costs. To protect consumers the FDA shouldn’t cut corners, they should devote more resources to the approval process of a drug that a manufacturer will agree to put on a distributed ledger.

Grant patent extensions. This will allow the manufacturers to sell drugs they develop at a premium for longer before generics can legally be sold that eat into their market share. It can be argued that this would hurt consumers since they would have to pay a premium for longer, but manufacturers could reduce price and maintain the same profitability since their volume sold would increase.

Mask the public keys associated with each distributed ledger participant. Keep all metadata encrypted inside of the blocks so that competitors can’t analyze the supply chain to gain competitive information. Auditors and regulatory bodies can be granted access to decrypt the information inside of a block in case of an audit or inspection [22].

6 Ethical Considerations

6.1 Traceability of Pharmaceuticals

Advertisers use labels like “organic”, “wild caught”, “sustainable sources”, “100% Colombian” to entice consumers to their premium brands. The reality is most of those claims can’t be substantiated. In fact, without DNA testing it’s difficult to tell if the white tuna ordered in a sushi restaurant truly is tuna or a cheaper substitute. Some of the blockchain projects above will prove if consumers are willing to buy brands with proven provenance and a traceable supply chain. Traceability of food sources will provide consumers with more choices. Traceability of luxury items may save insurance companies from fraud. Traceability of diamonds could reduce funds flowing to rebels in conflict zones who use them to finance their violence. In cases where there are human rights violations involved in the production of goods, the technology has the potential

to stop unethical and illegal practices, including slavery [20]. Traceability of pharmaceuticals is a matter of life or death. Counterfeit drugs cost lives around the world. In the US, we had the Heparin incident described above, but globally thousands of lives are lost when Malaria drugs are replaced with counterfeit drugs. As traceability is rapidly becoming a capability, ethically, we are bound to use these techniques to prevent criminals from tainting the prescription drug supply. While complying with the DSCSA will be difficult and expensive, it's also an ethically compelling concept, especially if it can be implemented globally.

6.2 Data Privacy

Perhaps the greatest ethical challenge facing data science today is the dual-edge sword of data privacy. When to keep data hidden and when to reveal or use data is not only a sensitive topic, it's one for which there are complex and changing global laws and growing consumer sensitivity. While patients may be willing to risk releasing their data into collections of population health data for the promise of longer and healthier lives, they may not want to release the same information for market research and the promise of more targeted advertising campaigns. It's an area where opinions on ethical behavior differ widely, leaving lots of 'gray' territory. Having the local pharmacy publish your prescription drug purchases in the Sunday Times is not ethical. Pharmacies legally sell data concerning prescription drug purchases, anonymized to a zip code, for market research. People with a rare disorder may feel the zip code is not anonymized adequately while others purchasing a widely-prescribed drug may not care. Having the analytic power to identify when \$40 million of opioids are shipped into a small market and holding those drug manufacturers accountable for the resulting explosion of opioid abuse would probably be considered an ethical application by most data science professionals¹⁴. Thus, our concept of 'ethical' treatment of data is based on how the data is used and data scientists must be informed not only about the laws but also about how the findings of any specific research effort might be used, even if the stated purpose seems noble.

DSCSA. DSCSA is not causing additional data to be collected or distributed for individuals. In fact, the dispensing of the drug pursuant to a prescription is explicitly excluded from the law. Thus, DSCSA does not represent incremental data privacy issues for individuals. What is at risk are the trade secrets and privacy of each participating business entity. Industrial espionage is real and exposing transactional patterns to the marketplace could be a threat to the participants' business. Thus, whatever data store is used must protect the participating entities from gaining unfair knowledge of inventory or trade practices of others in the supply chain. Since the point of DSCSA is to create transparency, this business need may be counter to enforcement of the Act. In this regard, blockchain offers some advantages because of the encryption. A blockchain does not easily lend itself to that type of analysis. The main requirement is to tightly control who would have access to the cryptographic keys as that capability

¹⁴ Wamsley, L. *Drug Distributors Shipped 20.8 Million Painkillers To West Virginia Town Of 3,000*. Available: <https://www.npr.org/sections/thetwo-way/2018/01/30/581930051/drug-distributors-shipped-20-8-million-painkillers-to-west-virginia-town-of-3-000>.

would unlock more ability to analyze the transaction data for patterns outside the stated purpose.

Blockchain. Likewise, the use of blockchain to meet the requirements of DSCSA does not present new data privacy dilemmas specifically relative to prescription drugs as the ethical dilemmas are common to all types of data that can be traced to individuals or communities. With that said, blockchain does present two unique data privacy dilemmas by nature of the technology.

First, blockchain data is ‘immutable’, it never goes away. Unlike an RDMS or any other data store, the data can’t simply be over-written with corrected information or ‘blanked out’. The data has to be updated with information in a new block and all subsequent reporting would need to read the entire blockchain or risk using incorrect data. The GDPR, which requires that EU citizens be able to request their personal information be removed from any data store, has implications for blockchain since it’s not possible to delete data. This is one reason why a lot of implementations don’t use blockchain alone. The blockchain is used to record the transactional information that should not change, but personally identifiable information that could change is normally stored in a more traditional data store with the link to that data encoded in the blockchain. In fact, since data in a blockchain is hashed, it can only be accessed and read by people who have the appropriate software to do so, which is why it’s viewed as a more secure data store. As many investors in Bitcoin have discovered, if you lose your private cryptographic key, your bitcoin is unrecoverable. Going deeper, what if the original ownership entry being reported by the blockchain is incorrect? What if the person populating the blockchain with property deeds simply replaces their name as the rightful owner? What if medical records recorded in blockchain record an incorrect diagnosis or treatment that was not provided to that patient? HealthCombix, in collaboration with PointNurse, is attempting to address this by introducing a service provided by nurses to ensure that the data entered into the immutable blockchain record is accurate and that the patient understands how to access, update, and grant access to their records [23]. More so than other data stores, the potential impact of incorrect data being instantiated into the blockchain must be considered by the designers with contingencies to address that occurrence built into the application if the data coming into the application could be wrong.

Second, because the data is encoded and parties to a transaction are obscured by the use of cryptographic keys, blockchain can be used to protect the identities of parties involved in criminal activities. Since a public blockchain has no centralized authority, there is no organization to serve a warrant to force disclosure of activity or identities. This has been an ongoing criticism of bitcoin and why it is so closely associated with the Dark Web. Decentralization is also why citizens in countries with corrupt banking systems are willing to trust Bitcoin instead of their state-governed bank. As with most technology, the ethical dilemma lies with the use case, not the technology.

7 Conclusion

When considering the viability of blockchain-based applications, most sources agree that the technology’s biggest barrier is simply that it’s too new. Regulations have not

been created. Technical understanding of the technology is limited and has not yet spread. Successful pilots have not been turned into successful applications at scale. However, last year, this same research group conducted a survey of literature for blockchain. At that time, there were a plethora of scholarly articles explaining blockchain and proposing applications for the new technology beyond cryptocurrency, mostly in the financial sector. This year, the articles have shifted to presentations and evaluations of pilot programs, with many articles presenting case studies on several different use cases relevant to supply chain. We discovered a wide array of pilot programs, including programs backed by significant industry leaders and global enterprise organizations like IBM, Wal-Mart, and Maersk, in addition to the expected array of start-up efforts. Most articles still predicted growth for the adoption of blockchain, even if they disputed the hype that blockchain would be an industry disruptor. We have demonstrated that blockchain, in theory, offers unique benefits to meet requirements for supply chain traceability. Yet, the technology is still unproven at the scale and performance that will be required to integrate into supply chain applications. While MediLedger's year-end statement is promising, their industry claims must be substantiated.

Certainly, the social climate supports traceability, if not the technology to achieve it. Consumers want more information about the provenance and traceability of foods so they will be more informed about quality and sustainability. How much more so would patients want assurances that their medications are safe and effective? With so much value in the pharmaceutical supply chain and the risk of death a real possibility, the cost justification is not difficult if traceability can prevent counterfeit or compromised drugs from reaching patients.

On the other hand, while blockchain offers promise, the current state of the supply chain industry may make adopting blockchain difficult. Blockchain is a data store. When coupled with IoT technology and smart contracts, it creates a compelling vision for a new paradigm, but what blockchain lacks is the thing supply chain needs the most to support automation: standardized data models. The supply chain industry is simply not prepared to adopt a shared ledger technology until/unless there is more commonality in how participants exchange data [24]. With that in mind, Modum may have the right approach. Instead of starting off with a full-fledged solution for drug traceability, solve smaller problems, gain experience, and build to a wider solution. Maersk seems to be taking the same "start small, gain experience" approach to their implementation. Focusing on the requirements for DSCSA, in essence, carves out a subset of the overall pharmaceutical supply chain functionality and allows focus on a portion of the problem with a stated data model.

2018 will be a pivotal year for blockchain adoption. As pilot programs end, organizations will decide if they are going to continue investing in the technology. Apparently, several key players recently confirmed that position. Forbes reported on a recent panel discussion about blockchain adoption from the technology community. Speakers included Anant Kadiyala, Director of Blockchain & Industry Solutions at Oracle; IBM's David Noller, Executive Architect Watson IoT - Blockchain and Industry 4.0; and Steven Kim, a Senior Director at SAP. The user community was represented by Jeff Denton, the Senior Director of Global Secure Supply Chain at AmerisourceBergen, one of the largest pharmaceutical distributors in the world. For a wide variety of use cases, Mr. Denton believes you start by assuming blockchain will

be the answer and only explore other technologies if you can prove blockchain doesn't work. According to Mr. Kim of SAP, "2018 will be a milestone year that we will see the adoption of a first set of blockchain solutions in enterprise applications - from securing the pharmaceutical supply chain to eliminating inefficiency in international logistics." Both Mr. Noller of IBM and Mr. Kadiyala of Oracle agree that 2018 will be the year that blockchain moves from pilots to everyday usage in business applications.¹⁵ Since DSCSA compliance is not required until 2023, that provides time for the market to gain experience and knowledge while blockchain technology matures.

8 Summary

By 2023, DSCSA requires the consistent traceability of pharmaceutical products from manufacturer to dispenser within the United States. Participants in the supply chain are expected to verify the chain of ownership, detect suspicious activity, and respond accordingly as outlined by the law. In addition, participants must be able to quickly respond to requests for information from enforcement officials. The final outcome of Title II will be the creation of an electronic, interoperable traceability system for pharmaceutical products at the package-level. The goal is to use real-time data capture to detect, respond to, and report potentially illegitimate drugs faster and more effectively before they can become a safety hazard to patients. The DSCSA was created to curb the circulation and sale of illegitimate pharmaceutical products. However, achieving this goal requires creating a reliable system of record with appropriate visibility to identify legitimate pharmaceuticals for all participants in the supply chain. Since members in the supply chain have compelling business reasons not to share information on inventory, a key challenge to ensuring compliance with traceability requirements will be establishing trust among stakeholders.

Blockchain applications are uniquely designed to provide traceability and to introduce trust into a trust-less system. As such, providing traceability of pharmaceuticals through the supply chain is a suitable use case for a blockchain implementation. This review demonstrated how a blockchain technology can provide functionality that benefits supply chain management in general and traceability of pharmaceuticals in particular. We identified several blockchain pilot programs relevant to traceability conducted by both global enterprises and start-up companies. However, none of these have the maturity to prove blockchain can operate at the scale required to support DSCSA compliance. Supply chain applications focused on compliance with track-and-track regulations like DSCSA may be the turning point for blockchain to prove it's worthy of the hype as an industry disruptor.

¹⁵ Banker, S. *The Growing Maturity Of Blockchain For Supply Chain Management*. <https://www.forbes.com/sites/stevebanker/2018/02/22/the-growing-maturity-of-blockchain-for-supply-chain-management/#24cb06bf11da>.

References

1. FDA. (2015). Drug Supply Chain Security Act (Title II of the Drug Quality and Security Act) Overview of Product Tracing Requirements. 2015. [Online]. Available: www.fda.gov/downloads/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/UCM464907.pdf.
2. Craighead, C., Blackhurst, J., Rungtusanatham, M.J., Handfield, R. (2007, February). An Empirically Derived Agenda of Critical Research Issues for Managing Supply-Chain Disruptions. *Decision Sciences, International Journal of Production Research* 43 (19), 4067-4081. Available: https://www.researchgate.net/profile/Robert_Handfield/publication/245330912_An_Empirically_Derived_Agenda_of_Critical_Research_Issues_for_Managing_Supply-Chain_Disruptions/links/5560d77808ae9963a119fa00.pdf
3. Christian L. Rossetti, Robert Handfield, Kevin J. Dooley. (2011). Forces, trends, and decisions in pharmaceutical supply chain management. *International Journal of Physical Distribution & Logistics Management*, Vol. 41 Issue: 6, pp.601-622. Available: https://www.researchgate.net/profile/Robert_Handfield/publication/235277709_Forces_trends_and_decisions_in_pharmaceutical_supply_chain_management/links/00b495214e2493d5f8000000/Forces-trends-and-decisions-in-pharmaceutical-supply-chain-management.pdf
4. Craighead, C., Blackhurst, J., Rungtusanatham, M.J., Handfield, R. (2007, February). An Empirically Derived Agenda of Critical Research Issues for Managing Supply-Chain Disruptions. *Decision Sciences, International Journal of Production Research* 43 (19), 4067-4081
5. Kun Yang, Haoting Shen, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. (2017 December). Hardware-Enabled Pharmaceutical Supply Chain Security. *ACM Transactions on Design Automation of Electronic Systems (TODAES)* (23, 2, Article 23), 26 pages. Available: <https://doi.org/10.1145/3144532>.
6. FDA.(2018). Definitions of Suspect Product and Illegitimate Product for Verification Obligations Under the Drug Supply Chain Security Act Guidance for Industry. 2018. [Online]. Available: <https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM598737.pdf>.
7. Rajgopal, Jayant. (2016) Supply Chains: Definitions & Basic Concepts. Department of Industrial Engineering, University of Pittsburgh. 2016. [Online]. Available: <http://www.pitt.edu/~jrclass/sca/notes/1-Overview.pdf>.
8. K. Korpela. J. Hallikas, T. Dahlberg. (January, 2017). Digital Supply Chain Transformation toward Blockchain Integration. Presented at Conference Hawaii International Conference on System Sciences (HICSS) 2017. [Online]. Available: <https://scholarspace.manoa.hawaii.edu/handle/10125/41666>
9. Attaran, M. (2007). RFID: an enabler of supply chain operations. *Supply Chain Management: An International Journal*. 12(4). 249-257. Available: https://www.researchgate.net/profile/Mohsen_Attaran/publication/216704130_RFID_An_enabler_of_supply_chain_operations/links/564cae9308acdda4c1343673.pdf.
10. FDA. (2018). Standardization of Data and Documentation Practices for Product Tracing Guidance for Industry. Available:

- <https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM598734.pdf>.
11. D. Yermack. (2016, November 28). Corporate Governance and Blockchains. Review of Finance. SSRN 2016. [Online] Available: <https://ssrn.com/abstract=2700475>
 12. Szeqczyk ,Pawel. Potential Applications of the Blockchain Technology in Healthcare. *Scientific Subjects Of The Silesian University Of Technology*. Volume 108. 2017.
 13. J. Lindman, V. K. Tuunainen, and M. Rossi. (Jan, 2017). Opportunities and risks of Blockchain Technologies in payments– a research agenda. Presented at Conference Hawaii International Conference on System Sciences (HICSS) 2017. [Online]. Available: <http://hdl.handle.net/10125/41338>
 14. A. Collob and K Sok. (3rd quarter, 2016). Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector? *Digiworld Economic Journal*. [Online] No. 103, p. 93. Available: http://www.academia.edu/30192464/Blockchain_Distributed_Ledger_Technology_DLT_What_Impact_on_the_Financial_Sector
 15. F. Glaser. (2017).Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. Presented at Conference Hawaii International Conference on System Sciences (HICSS) 2017. [Online]. Available: <https://scholarspace.manoa.hawaii.edu/bitstream/10125/41339/1/paper0190.pdf>
 16. Ryan, Philippa. (2017). Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain Technology. *Innovation Management Review*. October 2017. Volume 7, Issue 10.
 17. Apte, S., Petrovsky, N. (2016). *Will Blockchain technology revolutionize excipient supply chain management?* *Journal of Excipients and Food Chemicals*. September, 2016. Retrieved from <https://ojs.abo.fi/ojs/index.php/jefc/article/view/1465/1769>.
 18. Sternberg, H., Baruffaldi, G. (2018). Chains in Chains – Logic and Challenges of Blockchains in Supply Chains. *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 3936-3943). Available <https://scholarspace.manoa.hawaii.edu/handle/10125/50382>
 19. Francisco, K., Swanson, D. (2018). The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*. MDPI. 2, 2. Available: <http://www.mdpi.com/2305-6290/2/1/2/htm>.
 20. Kshetri, Nir. Blockchain’s roles in meeting key supply chain management objectives. *International Journal of Information Management*. 2018. Volume 39, pp 80-89.
 21. Bocek, T., Rodrigues, B., Strasser, T., Stiller, B. (2017). Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain. In *Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 772-777). Lisbon, Portugal.
 22. Kim, S.H. (2017). *The Drug Quality and Security Act of 2013: Compounding Consistently*. *Journal of Health Care Law & Policy*, (19, 2), 293-318. Retrieved from <http://digitalcommons.law.umaryland.edu/jhclp/vol19/iss2/5>.
 23. Engelhardt, Mark A. (2017) Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*. October 2017. Volume 7 Issue 10.
 24. K. Korpela. J. Hallikas, T. Dahlberg. (January, 2017).Digital Supply Chain Transformation toward Blockchain Integration. *Proceedings of the 50st Hawaii International Conference on System Sciences* (pp. 4182-4191).

Appendix

This project originated as a proof of concept. Our efforts failed, but in the interest of disclosure, we wanted to list some resources and methods we tried in hopes that it will help others. Initial efforts focused on using the Interplanetary Database (IPDB) which was touted as an internet-scale blockchain database. However, according to a post on ipdb.io in January 2018, “The world has changed, and funding to maintain and operate IPDB while maintaining its core values became an insurmountable struggle.”¹⁶ We speculate that funding may have dried up for IPDB due to the upcoming GDPR law.

Since ipdb.io cited that BigChainDB¹⁷ had been instrumental in their test network development, a combination of BigChainDB and MongoDB running in a Linux environment was next explored. While some limited success was obtained by following online documentation, we did not find the BigChainDB implementation had the ease of use required for the timeframe we were seeking to build the POC. Although BigChainDB seems to be a promising commercial product to build blockchains, the support is too expensive for an academic exercise and the open source implementation proved to be difficult.

After some searching for a simpler method, a Python tutorial was found on a blogpost at hackernoon.com that showed a straight forward method for building a blockchain. The code tutorial from the hackernoon article details how to build Rest APIs with Python libraries hashlib, json, and flask. The application operates using HTTP requests. The author of the tutorial suggests the use of cURL or Postman for testing the HTTP requests. Postman is cost prohibitive for testing due to the limited number of free transactions (1,000) while cURL did not interact well with Windows 10. We discovered an open source application named Advanced Rest Client which we used to test transferring data between the blockchain application and the client. While the code to read and write data was relatively straightforward, communication between nodes was unattainable.

Just after conclusion of our research, Amazon announced availability of their free blockchain templates. The authors recommend exploring those capabilities.

¹⁶ IPDB webpage. Retrieved from <https://ipdb.io/>

¹⁷ <https://docs.bigchaindb.com/en/latest/>