Journal of International Technology and Information Management

Volume 27 | Issue 3 Article 4

1-1-2019

Blockchain-Based Healthcare: Three Successful Proof-of-Concept Pilots Worth Considering

Rebecca Angeles
Univ of New Brunswick Fredericton, angeles.rebecca@gmail.com

Blockchain-Based Healthcare: Three Successful Proof-of-Concept Pilots Worth Considering

Rebecca Angeles
University of New Brunswick Fredericton, Canada
rangeles@unb.ca

ABSTRACT

This paper features the use of blockchain technology in the healthcare industry, with special focus on healthcare data exchange and interoperability; drug supply chain integrity and remote auditing; and clinical trials and population health research. This study uses the research method of analyzing the published case studies, academic articles, trade articles, and videos on MEDRec, Patientory, and the AmerisourceBergen/Merck alliance with SAP/CryptoWerk. The "blockchain" concept was introduced around October 2008 when a proposal for the virtual currency, bitcoin, was offered. Blockchain is a much broader concept than bitcoin and has the following key attributes: distributed database; peer-to-peer transmission; transparency with pseudonymity; irreversibility of records; and use of computational logic. The following three healthcare use cases have been taken up for proof-of-concept pilots by MEDRec, Patientory, and the AmerisourceBergen/Merck collaboration with SAP/CryptoWerk. While blockchain technology has a promising potential for specific use cases in the healthcare industry, there are major challenges to deal with as well.

KEYWORDS: Blockchain, Healthcare, Smart contract, Technology innovation, Distributed peer-to-peer networks

INTRODUCTION

This paper features the use of blockchain technology in the healthcare industry, with special focus on the following use cases: healthcare data exchange and interoperability; drug supply chain integrity and remote auditing; and clinical trials and population health research. Frost & Sullivan, a research organization specializing in information technology research, identified these promising use cases to pursue in the healthcare industry at this time (Frost & Sullivan (2017, June). This paper uses the proof-of-concept experiences of MEDRec, Patientory, and

ISSN: 1941-6679-On-line Copy

AmerisourceBergen in cooperation with Merck Co. to describe how blockchain technology might be successfully exploited in the healthcare industry at this time, with the current state of the technology.

This study intends to understand the state-of-the-art blockchain technology application in the healthcare industry, a very important domain in society. The initial deployment of the technology in the financial industry gave us a first glimpse into the possibilities with this technology for societal use. It is not the intention of this paper to describe basic blockchain technology in great detail, but rather to describe its accompanying components used in the first publicized proof-of-concept deployments in the healthcare industry. This paper also intends to drill down into the lessons we can learn from its most current organizational implementations.

The paper is organized accordingly. It opens with an introduction and literature review covering basic blockchain technology and use cases in the healthcare industry identified as most promising by Frost & Sullivan. The qualitative case study and content analysis methods are described in the research method section. Detailed studies of three use cases are presented in the findings section of the paper. The last section of the paper is the "Conclusions" section consisting of three parts: the first part features a table comparing Patientory and MEDRec, highlighting differences and similarities; the second part shows detailed lessons learned specific to the three organizations; and the last part discusses lessons of a more general nature that would apply to a wider range of healthcare blockchain implementations.

LITERATURE REVIEW

Blockchain Technology

Transactions in society between individuals and organizations are governed by contracts and records that describe the participation of certain stakeholders and details of the transactions that transpired. Entire economies depend on the tools that enable the capture, storage, distribution, and protection of these instruments. But there are issues to contend with in the presence of centralized entities that control these instruments involving trustworthiness, security, reliability of the information. While there is mistrust of intermediaries or centralized entities controlling these assets, there is also the paradoxical situation of separate siloed information systems that store this important information that have great difficulty exchanging data/information.

ISSN: 1941-6679-On-line Copy

The "blockchain" concept was introduced around October 2008 when a proposal for the virtual currency, bitcoin, was offered (Gupta, 2017). The bitcoin platform would eliminate a central authority for issuing currency, confirming transactions, and transferring ownership of the currency. Blockchain is not synonymous with bitcoin; it has many more business use applications besides digital currency and is the peer-to-peer network that is a layer above the Internet (Gupta, 2017). Table 1 explains the five basic principles underlying blockchain technology.

Table 1: Basic Principles of Blockchain Technology

Basic Principle	Explanation
1. Distributed Database	Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.
2. Peer-to-Peer Transmission	Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.
3. Transparency with Pseudonymity	Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.
4. Irreversibility of Records	Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they're linked to every transaction record that came before them (hence the term "chain"). Various

ISSN: 1941-6679-On-line Copy

	computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.
5. Computational Logic	The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between nodes."

Sources: (Gupta, 2017; Halamka, Lippman, & Ekblaw, 2017; Iansiti & Lakhani, 2017; Mainelli, 2017).

Three Promising Healthcare Use Cases

Frost & Sullivan (Frost & Sullivan, 2018, April 18; 2018, January; 2017, August 4; 2017, June; 2016, November) established the relevance, timeliness, and urgency of experimenting with blockchain in the healthcare industry due to the urgent need to cut costs, service a growing aging population with underserved needs, and increasing pressures from government to justify exponential healthcare costs in the years ahead.

Use Case 1: Healthcare Data Exchange and Interoperability

The first use case with maximum benefit potential is to use blockchain technology to enable healthcare data exchange and interoperability among different electronic healthcare record (EHR) or electronic record management (ERM) systems to serve the interests of the individual patient (Frost & Sullivan, 2017, June). Blockchain technology can address major dysfunctions currently experienced in the healthcare industry in the context of information exchange and system interoperability. Looking at relevant statistics in the U.S., about 46 percent of US clinicians have no access to the complete picture of their patients' records; conversely, US patients find it impossible to have a centralized and integrated view of their records and thus, are unable to share relevant information with care providers. With today's broken EHR and EMR systems, error rates for identifying records or integrating electronic files are as high as 25 percent for hospital and healthcare organizations, and higher even --- 50 to 60 percent --- outside of these systems. All these problems

cost US society about 150,000 lives and US$18.6 billion annually (Frost & Sullivan, 2017, June).

Blockchain technology can open up solutions to these challenges. First, patients can become more engaged with their health if they can gain access to cryptographically secure, irrevocable, and immutable historical and real-time data covering their in-patient, ambulatory, and remote patient monitoring (RPM) data. Just as importantly, care provider quick access to this data can significantly improve care coordination and manage emergency care situations. Second, the use of identity management using predefined user access rules in peer-to-peer networks can give patients the ability to share their anonymized healthcare data to support medical research and medical innovations. Third, important genomic and user-generated data, especially data generated by new technologies like mobile health apps and Internet of Things-supported healthcare devices and wearable computers can be captured and stored securely. Fourth, the blockchain network would override the previous siloed systems that prevented data/information exchange among different HER and EMR systems, and at the same time, reducing the costs and difficulty of data reconciliation among these systems (Frost & Sullivan, 2017, June).

Use Case 2: Drug Supply Chain Integrity and Remote Auditing

The pharmaceutical industry is beset with challenges in assuring its customers of the authenticity and non-tampering of its products. An estimated US$200 billion is lost annually in the global market due to fake drugs (Frost & Sullivan, 2017, June). In the European Union drug market, an average of US$33.5 million worth of drugs are stolen in cargo theft yearly. And about 30 percent of drugs sold in developing countries are counterfeit products. In a related vein, outsourcing pharmaceutical contract research and manufacturing services globally spawns a wide range of administrative, legal, ethical, financial, and staff-related concerns. In outsourcing the manufacturing drug products, greater risks are incurred in offloading production in a foreign country where controls may be more likely to be nonexistent. It is more important to use tools to enable supply chain provenance and chain of custody from the time raw materials are acquired from suppliers through to production, distribution by the wholesaler, pharmacist (i.e., retailer), and final consumption point with end customers. Using blockchain technology, an immutable hash is used to automate the serialization and geo-tagging process throughout all the steps involved --- R&D tasks, testing, and production in manufacturing facilities. The process of serialization uses a system to track and trace the movement of prescription drugs through the supply chain, identifying each product using the following information --- unique serial number, product origin, shelf life, and batch number (Chatterjee, 2015, January 20).

ISSN: 1941-6679-On-line Copy

Blockchain "smart contracts" can also be used to automate the auditing of outsourced contract manufacturing of drug products and quality compliance by the manufacturer. Smart contracts can also be used for autonomous applications for due diligence, inventory management, and product recalls. Blockchain also enable the creation of proof of identity (or license) of drug products and immutable records which regulatory agencies could use to cut back the inflow into the country of counterfeit drugs and identify sources of compromised products. A reporting system can also be established in order to inform citizens of adverse drug reactions associated with drug products. Blockchain can improve the pharmaceutical supply chain financial transactions by facilitating the authenticity of transactions involving drug products, lowering credit risk, and speeding up payment cycles (Frost & Sullivan, 2017, June).

Use Case 3: Clinical Trials and Population Health Research

The current IT infrastructure undergirding the healthcare industry makes it difficult to report and share clinical trial results. An estimated 50 percent of all clinical trials are unreported and as a rule, healthcare researchers/investigators are unable to disseminate their study results (Frost & Sullivan, 2017, June). In the specific case of ClinicalTrials.gov, about 90 percent of the trials even lack results. This creates an impoverished situation where the growth of healthcare knowledge capital is hindered, leading to serious health risks to society as a whole.

Blockchain technology can be used for a number of scenarios to benefit clinical trials and population health research. First, clinical trial protocols and results could be time stamped and render them immutable. Second, patients can grant access to their personal health records securely to researchers and pharma clinical trials through the use of eConsenting and smart contracts. Third, the clinical trial patient recruitment process could be more targeted using the eConsenting feature and gaining access to anonymized universal health records. Fourth, new models like the use of research commons and renumerative models can be used to encourage data sharing and allowing access to anonymized medical metadata in the form of transaction fees for research use cases. Fifth, blockchain technology can address the issue of "fraud" in medical research resulting in outcome switching, data snooping, and selective reporting --- all nefarious activities --- by assuring clinical trial integrity and enabling provenance of medical data trails (Frost & Sullivan, 2017, June).

ISSN: 1941-6679-On-line Copy

RESEARCH METHOD

While there are numerous articles on the potential of blockchain technology in the healthcare industry, there are fewer papers on the successful pilots conducted thus far. Therefore, it is the main objective of this paper to provide a descriptive reporting and understanding of three prominent case studies that have reached successful proof-of-concept stage in the experimentation with blockchain technology. The three use cases were identified by Frost & Sullivan Research (Frost & Sullivan, 2017, June) as the most promising areas to be exploited at this time in the healthcare industry. Published case studies and related academic journal articles and trade articles were content analyzed, along with videos on MEDRec, Patientory, and SAP/CryptoWerk collaboration for blockchain in the pharmaceutical industry.

FINDINGS

Patientory

As a Software as a Service firm, Patientory, offers a blockchain-based distributed application that enables patients, clinicians, and health organizations to access, store, and transfer information to meet patient needs and improve healthcare coordination among various institutions (McFarlane et al., 2017; Patientory, 2017a, June 20; Patientory, 2017b, July 24; Gaskell, 2017, May 3). Patientory provides a platform for these entities to interact and communicate easily as it interconnects electronic medical record (EMR) systems such as Epic, Cerner, Allscripts and Meditech and other health related database systems. The SaaS firm also offers patients a mobile app they can use to capture health-related data from both traditional and non-traditional sources (i.e., FitBit, etc.) and create their personal profiles, stored in secure HIPAA-compliant servers. Encouraging greater patient engagement with their health, the app can also be used by patients to contact their care providers and other patients with similar health issues.

Patientory was designed to address the major limitations of the healthcare system as it currently operates in the U.S. The patient-centered enterprise software solution acts as an intermediary to the many siloed, fragmented, and centralized electronic medical record (EMR) keeping systems (Becker's Health IT & CIO Report, 2017, January 19; Bitcoin Magazine (n.d.); Cohen, 2017, August 31; Health Transformer, 2017, August 29; Ribitzky et al., 2018).

ISSN: 1941-6679-On-line Copy

In order to do this, Patientory uses: (1) encrypted middleware to meet high-volume transaction exchanges in the healthcare industry; (2) application programming interfaces (APIs) to facilitate speedy information exchange and transfer; and (3) HIPAA-compliant health information storage assets that observe geography-specific regulations (McFarlane et al., 2017).

Patientory uses the Patientory token (PTOY) to support its operations (McFarlane et al., 2017; Patientory, 2017a, June 20; Patientory, 2017b, July 24). Once patients subscribe for the service, they are given an allotted amount of space to store their personal health information for free. They may purchase additional PTOYs using the platform or an exchange to enable them to purchase additional storage space in the nodes set up in hospital systems. The PTOY also used by healthcare organizations which sign up for the SaaS via service contracts. Healthcare organizations use the PTOY to pay for the creation and execution of smart contracts and transactions. Patientory also incentivizes large healthcare organizations that possess large server storage space to trade PTOY tokens with small- and medium-sized healthcare organizations interested in gaining access to the blockchain healthcare network without incurring the costs of implement nodes themselves. Overall, the PTOY regulates Patientory's network storage allocation, healthcare quality measures, and revenue payment cycles.

Other sources of revenue for Patientory include fees from providing technical support and population health management services as a result of using machine learning and aggregating data on the blockchain platform that provide physician diagnosis support, patient-care provider care coordination, and patient engagement. Patientory uses the Ethereum Blockchain platform that applies a Turing complete programming language executed on the Ethereum Virtual Machine. Oracle Services are used to allow the Virtual Machine to interact with the Internet (McFarlane et al., 2017).

Patientory uses a private implementation of the Ethereum blockchain which is a permissioned blockchain. It consists of a network of blockchain nodes that can interact only with other blockchain nodes, a key authoring entity, the HIPAA compliant storage facility, and the remote procedure call (RPC) server. Public and private key pairs to be used in the blockchain are generated by the key authoring entity. The electronic private health information (ePHI) is stored by the HIPAA compliant data storage facility (McFarlane et al., 2017).

The Patientory system contains three class level objects: the institution, the institution's employees, and customers (i.e., patients). The "individual class contract" embodies information that indicates that every user maps to a private

address on the private blockchain. Also, each private address is authorized to speak to one contract in the blockchain. The "institution contract" lists the customers (i.e., patients) who have granted permissions for viewing privileges to select institutions. This institution contract also lists its authorized employees. The "customer contract" lists all the institutions patients have granted viewing permissions to. The steps involved are (McFarlane et al., 2017):

1) A requesting entity issues a request for information; this request is a cryptographically signed transaction which is sent to the remote procedure call (RPC) server. This RPC server verifies the identity of the requesting entity using the signature in the login request.
2) The database of permission login public keys receives the signature from the RPC server and checks if there is a matching entry in the database. If there is a match, this database sends a message to accept the request.
3) The RPC server also sends a copy of the incoming request to the data aggregation server, which, then, forwards this request to miners based on a load sharing mechanism.
4) The miners sends the request to the requesting party's controlling contract, which contains information on the permissions to access specific pieces of data that the requesting part is authorized to access. If the controlling contract indicates the permission to access the information requested, then, the incoming request is deemed valid.
5) The controlling contract has a system of hashed pointers that lead to requested information. The controlling contract sends an event message to the HIPAA storage server, which contains the data and resolves the system of hash pointers. The controlling contract executes as valid request transaction which, in effect, activates the blockchain event messaging system, which contacts the HIPAA forwarder.
6) The HIPAA forwarder recognizes the valid request and creates an encrypted request against the HIPAA storage server based on the hashes of the event message, which contains the public key of the requesting party.
7) Also, the data aggregation server sends the request to the private blockchain verifiers, which compare the information request against a "target contract." If the information request is deemed valid, then, the transaction is entered in the next block of the block chain via the mining process. An event message in the blockchain is also generated.

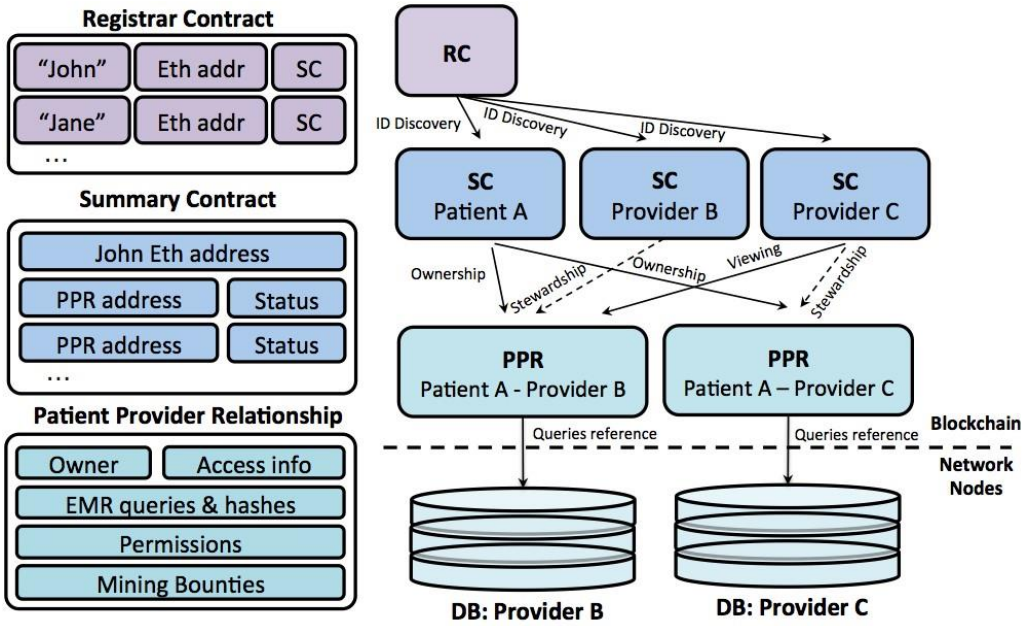
ISSN: 1941-6679-On-line Copy

MEDRec

MEDRec is the product of the collaboration of the MIT Media Lab and the Beth Israel Deaconess Medical Center, along with the individuals, John Halamka, Ariel Ekblaw, Andrew Lippman, and Asaph Azaria, to pilot a blockchain-based record management system to process electronic healthcare records (Ekblaw, 2017, 2016; Halamka et al., 2017; Azaria et al., 2016). MEDRec was not designed to store patients' health records; instead, it stores the signatures of the patients' records on the blockchain network and alerts them when transactions are initiated (Halamka et al., 2017). The system is also designed to empower the patient as the locus of control in managing the flow of transactions on the blockchain.

The MEDRec system uses three types of contracts: the registrar contract (RC), the patient-provider relationship contract (PPR), and the summary contract (SC) (Figure 1).

Figure 1: Three Contract Types in MEDRec System



Sources: (Azaria et al., 2016; Ekblaw et al., 2017; 2016)

The Registrar Contract

The registrar contract is also the global contract used to map participant identity strings to their Ethereum address identity, which is equivalent to a public key. This contract contains policies that manage the registration of new identities or modification of the mapping of existing identities. Only certified institutions can be processed via identity registration (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

The Patient-Provider Relationship Contract (PPR)

The patient-provider relationship contract can be implemented in any pairwise data stewardship interaction and is issued between two nodes in the system where one node manages medical records for the other node. The following is a description of how the PPR behaves in the context of a healthcare provider's database. The PPR defines the data pointers and associated access permissions that identify the records in the healthcare provider's database. Every time a query string is executed in the provider's database, the pointer associated with the query returns a subset of a patient's data. The system is designed to assure that no alterations to the data at the source have taken place through the use of a hash affixed to the query string. Using the hostname and port information, the location of the provider's database in the network is given to enable access to it. The healthcare provider designs the data queries and modifications to these queries whenever new records are added to the database (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

To enable patients to share their data with others, a hash table has been designed that maps third parties' addresses to a list of additional query strings, which indicates the portion of the patient's data a specific third party is allowed to view (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

The Summary Contract (SC)

The SC holds a log of all interactions between a patient and care providers and other third-party institutions authorized by patients to access their data. Likewise, the SC holds a log of transactions between care providers and patents and all third parties allowed by patients to access their information. The SC blockchain log, therefore, contains histories of the participation of patients, care providers, and healthcare organizations in various past and current interactions involving nodes in the blockchain network. The system is designed to ensure that the SC blockchain logs are maintained, backed up, and restored in cases of system crashes (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

ISSN: 1941-6679-On-line Copy

The SC also enables notifications to be sent to patients regarding the status of transactions. As a rule, care providers update patients' records and could add new relationships in these records. Patients, therefore, could consult their SCs and find notifications about new relationships being suggested to them or updates to their SC logs. Patients have control in the sense that only they can accept new relationships being presented to them, and reject or delete these relationships --- deciding which records in their SC log they would like to acknowledge. Patients may also leave the blockchain network many times and later, rejoin it. They may gain access to their history with the blockchain network by downloading the latest blockchain in the network (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

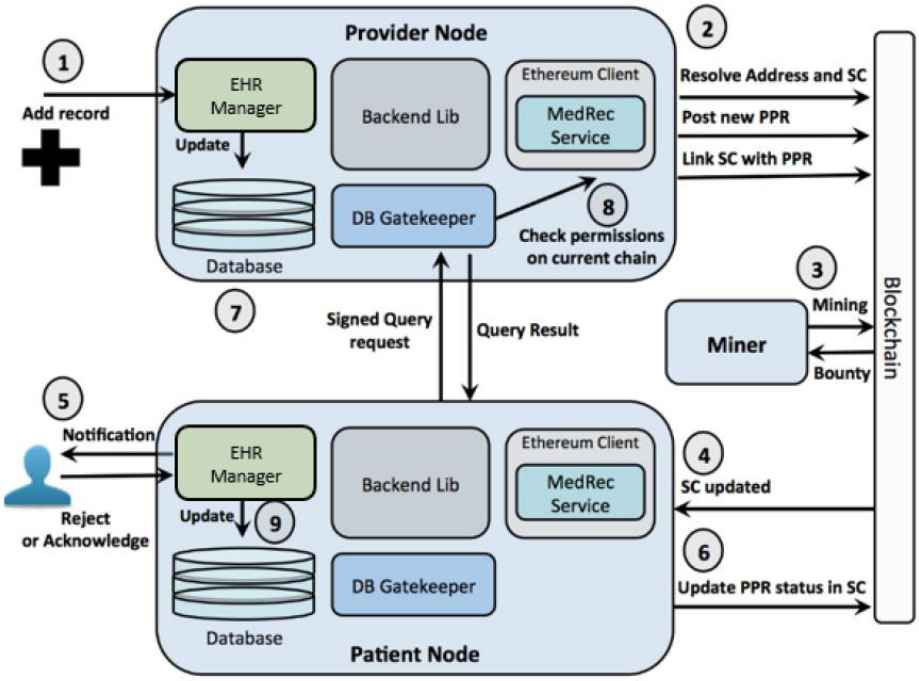
The MEDRec system also works with four software components stored in servers: backend library, Ethereum client, database gatekeeper, and EHR manager (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

The Backend API Library

MEDRec was designed to facilitate the interactions between external health record management applications and the blockchain network using a "backend API [application program interface] library." This library is a bundle of various utilities written to handle "hurdles" in interacting with the blockchain network such as verifying transactions so that they are accepted with high confidence by the network. Examples of other "hurdles" include handling uncertainties associated with transactions that are mined and managing transactions that are discarded. This backend API library uses the Ethereum client to deploy low-level formatting and parsing of the Ethereum protocol (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

Steps 1 and 2 in Figure 2 shows the tasks involved in a sample scenario involving a healthcare provider adding a record in the blockchain network for a new patient. First, the patient's identification information has to match an Ethereum address and the associated summary contract needs to be found. Then, the healthcare provider establishes its stewardship of the data owned by the patient's Ethereum address by uploading a new PPR to the blockchain network. Afterwards, the provider node creates a query to reference this patient's data, update the PPR, and link this PPR to the patient's summary contract. This will, then, allow the patient node to locate it later on the blockchain network (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

Figure 2: Interactions of MEDRec Software Components



Sources: (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

Ethereum Client:

The Ethereum client undertakes all the tasks involved when a participant joins the blockchain network. So, for instance, the client will connect a participant to the peer-to-peer network, encode and send transactions, and keep a verified local copy of the blockchain. The client has been modified so that it is aware of the mapping of a participant identity and its associated Ethereum address. The client also uses the registrar contract address lookup function in order to locate the node's summary contract. The client does this constantly as a way of monitoring real-time changes to the summary contract. If an update transaction occurs, the client will alert the electronic healthcare record (EHR) manager to send a user notification and if needed, to sync the local database (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

The patient perspective is taken in describing steps 4 to 6 in Figure 2. The patient's Ethereum client monitors his/her summary contract constantly. This patient is notified by the client when a new block is mined with the newly linked PPR. At that point, the patient decides whether or not to acknowledge the transaction with a

ISSN: 1941-6679-On-line Copy

provider --- in either case, the summary contract is updated with the result of the decision. If the patient accepts the provider transaction, a query request is generated in order to get new medical data. This query uses the information in the new PPR to find the provider on the network and link with its database gatekeeper server.

Database Gatekeeper:

The database gatekeeper manages the off-chain access interface to a node's local database, in keeping with permissions recognized in the blockchain network. A server, under the gatekeeper's supervision, listens for query requests from clients on the network. Issuers of these requests cryptographically sign the requests to enable the gatekeeper to confirm the issuers' identities. Such requests contain a query string and a reference to the associated blockchain PPR warranting permissions to run the query. If the issuer's signature is certified, that is, if their identities are confirmed positively, then, the gatekeeper checks the blockchain contracts to verify if the address associated with the request has permission to access the query. If the address is allowed access, then, the gatekeeper runs the query on the node's local database and sends the resulting data to the client (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

Finally, steps 7 to 9 in Figure 2 describe how a patient obtains personal data from a provider node. The mechanics are similar to the steps involved when third parties try to obtain patient-shared data. First of all, the patient needs to determine the data he/she is willing to share with a specific third party and updates the associated PPR with that third-party's address and query string. When needed, the patient's node can use the registrar contract to resolve the specific third party's address on the blockchain. Afterwards, the patient node will link its existing PPR with the care provider onto the specific third party's summary contract. As a result, the specific third party will receive notifications of new permissions issue and using the link, will be able to locate requested information. The provider's database gatekeeper will recognize the new permissions granted to the specific third party and confirm that the patient issued the permissions on the PPR they share with this patient.

EHR Manager:

The EHR management and user interface (UI) application, accessed through a Web interface, gives end users the point of contact with the blockchain network. This application enables end users to view the system, receive update notifications, share data, and retrieve data. The Python backend framework was used to build this UI application, which has a built-in compatibility for the use of mobile devices as well (Azaria et al., 2016; Ekblaw et al., 2017; 2016).

The MEDRec network uses Ethereum's cryptocurrency, Ether, to incentivize work on the blockchain network and secure itself using proof-of-work mining (Blockchain Dummies, p. 58). Ether is used to execute code associated with smart contracts in an Ethereum blockchain network. MEDRec has two incentivizing models for encouraging work in its blockchain. The first model will encourage participants to use Ether, which can be won by mining and winning participants will gain an acceptable amount of Ether to the node that solves the computational puzzle. Care providers are encouraged to perform mining to support their activities on the MEDRec blockchain such as posting and updating PPRs, accepting viewing permissions, among other transactions. Patients will also need Ether if they want to conduct transactions such as sharing their health data with other third party organizations, or having the latter pay for such transactions. Healthcare regulations often determine who has to pay.

The second incentivizing model specifically addresses medical researchers, who will be encouraged to conduct mining activities in order to gain access permissions to aggregate anonymized medical data from patients, care providers, and other healthcare organizations. The MEDRec blockchain network designed a feature in the PPR wherein care providers are required to attach a bounty query to any transaction they issue updating the PPR. To illustrate this mechanism, here is an example: a bounty query can be formulated to return the average cholesterol levels in blood tests conducted by a care provider across all patients for a certain 30-day period. When the block containing this transaction is mined, the function automatically appends the winning block miner as the owner of the bounty. This miner, then, collects the bounty by issuing a request to the care provider's database gatekeeper. This request is also signed by the provider as part of the transaction, thus, ensuring that the bounty query has not been maliciously altered.

AmerisourceBergen and Merck Co. (SAP/CryptoWerk Alliance)

Major healthcare organizations, AmerisourceBergen, a drug wholesaler and drug developer Merck & Co. are collaborating in using blockchain technology (Antonovici, 2018, June 8; CryptoWerk 2018b, 2018c). The following objectives are important to these organizations in their use of blockchain: (1) establish the ownership of the drugs throughout the supply chain; (2) verify the fact that drugs delivered to customers or returned to the wholesaler or manufacturer have not been tampered with; and (3) comply with current and new healthcare industry regulations that will take effect in 2019 that address the identification of fake, stolen, or contaminated drugs in the supply chain (Antonovici, 2018, June 8).

ISSN: 1941-6679-On-line Copy

A key driving force for blockchain adoption are regulatory requirements like the 2019 deployment mandate of the Drug Supply Chain Security Act (DSCSA) in the U.S. (Bylo, 2017, April 7). By November 2019, wholesalers are required to verify unique product identifiers of pharmaceutical goods and accept only serialized products. Pharmacists are expected to do the same a year later ---- November 2020. Both wholesalers and pharmacists, however, must give access to information that will reveal the ownership of pharmaceutical products back to the original manufacturer or repackager --- by November 2023.
Earlier DSCSA mandates involved requiring manufacturers, wholesalers, repackagers, and pharmacies to deploy lot level management as of 2015. By November 2017, the DSCSA required the use of product identifiers (GS1 Global Trade Item Number [GTIN®] or the Food and Drug Administration (FDA) National Drug Code [NDC], serial number, lot number, and expiration date embedded in a DataMatrix barcode --- to be used in serializing drug products (Bylo, 2017, April 7).

AmerisourceBergen and Merck are using the integrated SAP solution that combines the CryptoWerk Enterprise Blockchain Enablement Kit and the SAP Advanced Track and Trace solution (CryptoWerk, 2018a, 2018b, 2018c, 2018d, 2018e; Hecker, 2018, June 15).

SAP Advanced Track and Trace solution

AmerisourceBergen and Merck are using the SAP Advanced Track and Trace solution in conjunction with the CryptoWerk Enterprise Blockchain Enablement Kit. The use of the track and trace solution is a direct response to the need to comply with country-specific legal requirements on serialization, tracking and tracing, and regulatory reporting of pharmaceutical products (SAP, 2018, April 6). This software solution also facilitates the exchange of data/information with supply chain trading partners. Serial number events associated with pharmaceutical products (i.e., medicinal sales units and their aggregations; batches and their serial number relations) can be reported to regulatory agencies and supply chain trading partners in compliance with regulation requirements. These serial numbers are captured from packaging lines and warehouse systems and are stored centrally. The solution can also report on the usage and distribution of serial numbers globally --- this is important as country-specific legislations have different requirements in terms of serial number management. This usually involves serial number definition in terms of length and character set, randomization, data capturing, and data exchange with trading partners. The track and trace solution integrates with native enterprise resource planning (ERP) systems, warehouse management systems, and packaging lines the firms might have.

ISSN: 1941-6679-On-line Copy

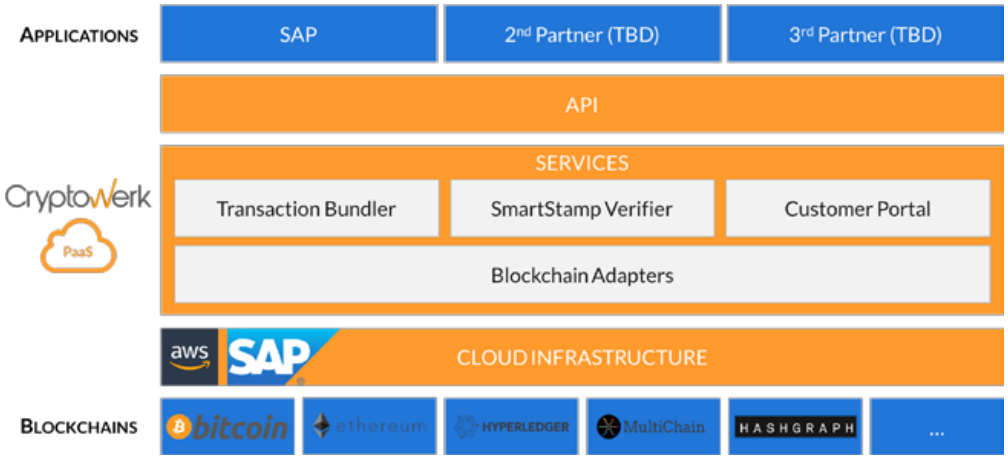
CryptoWerk Enterprise Blockchain Enablement Kit

CryptoWerk offers an SAP-certified blockchain-based solution that can firms involved in the pharmaceutical industry can use to offer assurance that their products have not been tampered with along the supply chain (Hecker, 2018, June 15; CryptoWerk, 2018d, 2018e).

The CryptoWerk kit enables data interoperability between disparate network of applications (CryptoWerk, 2018a, 2018b, 2018c) (Figure 3). Participating firms can have data interoperability between disparate network applications using the CryptoWerk kit and also use various application languages. The kit can also connect participant firms with any public, private, or hybrid blockchain networks. The following are the different components of the CryptoWerk enterprise blockchain enablement kit (CryptoWerk, 2018a, 2018b, 2018c):

1. CryptoWerk Engine;
2. CryptoWerk REST (representational state transfer) API (application program interface), used for inserting and retrieving data to and from the engine;
3. A universal blockchain connector, that provides the ability to use any or many blockchains

Figure 3: CryptoWerk Blockchain Enablement Kit Platform



Source: (CryptoWerk, 2018b, p. 7)

This is how the CryptoWerk kit works (CryptoWerk, 2018b). First of all, CryptoWerk does not store original customer data on blockchains. In submitting a transaction or file to the CryptoWerk server, a client/participant needs to hash this

ISSN: 1941-6679-On-line Copy

digital asset and include identifying metadata. CryptoWerk will confirm receipt of the hash by responding to the client with a ticket number. CryptoWerk, then, bundles collected hashes from all its clients and will generate a single bundle hash called an "anchor."

The client indicates the blockchain/s to which their digital assets should be sent. Using the ticket number, CryptoWerk sends the anchor to the target blockchain server for validation.

These blockchains, in turn, confirms specific transactions and the position of the anchor in the blockchain. When this happens, CryptoWerk issues a "SmartStamp" --- this is proof of authenticity of the transaction or document --- to the client. The following items constitute the "SmartStamp": a calculation instruction, the hashed transaction or document, and the anchor or hash of the bundled transactions. Only one SmartStamp is issued per blockchain; the client, of course, could be submitting a transaction/document to multiple blockchains.

Clients can present the "SmartStamp" to their trading partners in the supply chain and use it as an irrefutable proof of their products' existence and authenticity in the respective blockchains.

CONCLUSIONS/LESSONS LEARNED

This section will discuss lessons learned for each of the three firms and resulting conclusions for each as well. Finally, general lessons for blockchain deployment as a whole will be presented as well.

Table 2 shows a quick comparison of Patientory and MEDRec, highlighting the key differences and similarities between the two. The details of the entries in the table of comparison are discussed in the respective subsections devoted to these firms and the lessons learned sections as well for both firms. The AmerisourceBergen/Merck blockchain is not included in the table as it is clearly a different blockchain implementation involving the pharmaceutical industry supply chain.

ISSN: 1941-6679-On-line Copy

Table 2: Differences and Similarities Between MEDRec and Patientory

Part A: Differences

DIFFERENCES		
Attribute	**MEDRec**	**Patientory**
-deployment architecture of blockchain network	-more of a private, permissioned blockchain	-B2B2C blockchain network; is a hybrid ecosystem with aspects of both private and public networks
-development team behind the blockchain network	-developed by MIT Media Lab & graduate students	-developed by Patientory IT employees
-stage in blockchain network evolution	-still early stages: completed MEDRec 1.0 proof of concept; currently working on MEDRec 2.0 version	-further along with roadmap; in late 2018, completed a survey of beta users of its mobile app for personal health; majority of sample respondents are very satisfied with mobile app; Patientory has yet to publicize organizational level pilot projects conducted
-location for storage of blockchain data	-data NOT stored in blockchain network	-data IS stored in blockchain network
-other institutional support for the blockchain network infrastructure	-no institutional support yet for IT infrastructure	-IT infrastructure supported by Patientory Stiftung (Germany)
-institutional collaborations participated in to support blockchain network	-not as networked as Patientory; still in early stages and its platform is still being developed further and improved	-actively working on institutional collaborations: DASH, BlockCypher, Startup Health, HyperLedger, Ethereum, etc.
-focus on medical research	-strongly supportive of medical research	-medical research is not a key focus
-blockchain mining incentives and required epayments for network services	-medical researchers will be rewarded with anonymized patient data for research and analysis if they undertake data mining to support the blockchain network;	-PTOY used by patients to purchase patient data storage space in Patientory; healthcare organizations are charged a monthly licensing fee for network & consulting services -other digital currencies accepted
-data mining conducted on the network	-plans to eliminate current mining methodology in the future; for MEDRec 2.0, will use a substitute	-no plans of eliminating mining

ISSN: 1941-6679-On-line Copy

	method for supporting the blockchain network	
-management of patient-generated health data	-does not yet handle user-generated medical data (e.g., via FitBit)	-has developed a mobile app for personal health & completed an end user beta survey late 2018 -plans to accept user-generated health data such as data generated by its mobile app and other tools like FitBit

Part B: Similarities

SIMILARITIES		
Attribute	**MEDRec**	**Patientory**
-use of Ethereum platform for smart contracts	-Ethereum based	-Ethereum based
-support for open source development of blockchain network	MEDRec was designed with flexibility to support open standards for health data exchange	-Patientory will integrate its blockchain with HyperLedger's open source code.
-recipient of institutional support in early stage of development	-had early stage institutional backing and pilot tested with Beth Israel Deaconness	-had early stage institutional backing and pilot tested with Kaiser Permanente
-deployment architectural type	-private, permissioned blockchain	-has aspects of a private, permissioned blockchain

Lessons Learned: Patientory, Inc.

Patientory, a venture start-up firm, offers blockchain network based-services using the B2B2C business model and lessons learned for this organization are very different from those for MEDRec, even if some of their services overlap in nature.

Patientory's top management has made it a point to reach high visibility in the marketplace via social media and traditional channels and appears to have successfully done so. In September 2018, Medtech Insight, a provider of real-time news and analysis for medical device and diagnostics professionals, recognized Chrissa McFarlane as the "Entrepreneur of the Year" (Patientory, 2018, September 23). The Medical Futurist (TMF) named Patientory as one of the most promising

12 top firms introducing innovative technologies like blockchain in digital health (The Medical Futurist, 2018, March 27). In November 2017, Patientory won two prestigious awards granted in the state of Georgia: the Phoenix Award for Start-up Company of the Year and was named the Health Tech Upstarter in the Technology Association of Georgia Awards event (Patientory, 2017, November 7). The firm won the top prize in the 2017 Southeastern Medical Device Association Conference (SEMDA) as well (Patientory, 2017, May 3).

Patientory has been proactive in seeking collaborative engagements that would support the firm. First of all, Patientory, Inc. is supported by Patientory Stiftung, a Swiss non-profit organization that provides the blockchain technology infrastructure to the firm (Patientory, 2018, March 1). The firm also conducted an initial pilot program in cooperation with Kaiser Permanente involving about 25,000 patient records for chronically ill patients (McKesson Ventures, 2017, May 10). Patientory also joined a new grant program involving DASH, an epayments exchange that supports digital currencies, and BlockCypher, a blockchain web services provider (Patientory, n.d.a). The firm received a grant from both companies that funded the integration of Dash epayment services with Patientory, using BlockCypher's application program interfaces (APIs). BlockCypher's services will also help Patientory become interoperable with other healthcare blockchain networks. Patientory also joined Startup Health, a networked community that promotes and supports entrepreneurial health "transformers" who introduce innovative/breakthrough health products and services.

Patientory seeks to stay abreast with the latest developments in blockchain technology and has joined both the Ethereum and HyperLedger tech communities. By partnering with HyperLedger, Patientory will integrate its current blockchain with HyperLedger's open source code (Patientory, 2017, August 29).

In terms of raising financial support for the firm, Patientory has secured around U.S. $7.2 million from PTOY currency buyers (Patientory, 2017, June 3).

At this time, Patientory appears on track towards a full blown deployment of their business model. The results of a recent survey of end users of Patientory's mobile Dapp signal a very positive reception of the firm's services for individual customers. These are the highlights of the survey. Patientory conducted a survey of users of the "VIP beta version" of its health tracking mobile app for the period May 31, 2018 through to August 26, 2018 (Patientory, 2018, August 28). The goals of the survey were: (1) to see if the mobile app is effective and working as intended; (2) to see if users like the end user interface and have them evaluate its general quality; (3) to test how the app functions in real-world user environments; (4) to

ISSN: 1941-6679-On-line Copy

test the goal-setting, activity tracking, and wallet features of the app; (5) to test the data storage protocols used for securing personal health information gathered during the test period; (6) to test the IT infrastructure support behind the apps; and (7) to collect user testimonials and suggestions for future improvements.

Eighty individuals participated in the survey, most are affluent and live mainly in the U.S. (i.e., urban dwellers in New York City, Atlanta, San Francisco, and Los Angeles), United Kingdom, Australia, New Zealand, and Switzerland.

Briefly, selected survey findings worth noting are the following. Seventy percent of the participants found the mobile app easy/intuitive to install on their mobile phones. A good part of the sample said they used the app for setting goals for walking and exercise. Eighty percent tracked their walking exercises; sixty percent tracked their food intake and hydration. About 50 percent tracked their body system measures. More than 33 percent are athletic. About 33 percent tracked their weight training. Twenty percent tracked their running activities and another twenty percent tracked their swimming. One third of the sample tracked specific health conditions on account of their chronic illnesses. Only 10 percent tracked the medication they used and purchased. Only 30 percent used an electronic health record portal at the time of the survey. A significant 80 percent used the PTOY wallet feature of the mobile app. And 75 percent own other digital cryptocurrencies or tokens aside from PTOY. More than 50 percent use digital wallets like Coinbase, Apple, Jaxx, myetherwallet, etc. About 30 percent thought there was no need to add features to the mobile app. Suggestions for future improvements include medication tracking specifically for allergies, reminders for regular health maintenance, additional health tips, diet tracking, and data visualization improvements in terms of using graphs for weight and heart rates.

A related challenge is motivation on the part of the individual customer stakeholders. To maintain a blockchain network infrastructure, an organizational stakeholder has to commit computing resources and a large number of independent nodes to conduct mining activities. Meanwhile, the computer infrastructures of existing hospital and healthcare organizations usually have a small number of nodes in their respective networks. An individual stakeholder like a patient, on the other hand, would have to do the following: (1) buy or rent sufficient computing resources to undertake mining activities; (2) learn how to use cryptocurrencies in order to purchase tokens like Ether or PTOY in order to participate in the blockchain; and (3) learn how to recognize, interpret, and use alerts and messages from the blockchain network. All three requirements demand a certain level of computer literacy and possession of wherewithal to support participation in the

ISSN: 1941-6679-On-line Copy

blockchain network which may not be available to low-income or the computer illiterate segments of the population.

There are as yet no published results of pilot projects conducted with potential organizational clients, nor are testimonials from this type of client shown on Patientory's website.

Patientory recognizes that it must gain traction with healthcare organizations, who are their main customer targets for their software as a service offering (Patientory, 2017a, 2017b). One way to do this would be to seek to partner with care providers, primary care physicians, hospitals, etc. In the future, Patientory intends to offer benefits derived from the application of artificial intelligence and machine learning to its clients. Using these assets, Patientory should be able to make more accurate medical diagnoses and treatment recommendations that care provider can use, for instance (Patientory, 2017a, 2017b). Patientory also intends to capitalize on their mobile app platform that should serve the needs of individual patients whom it will incentivize to have a more proactive role in disease prevention using their smartphones and also encourage the use of wearables like FitBit bracelets for monitoring their health status (Marr, 2018, January 25).

Since Patientory is a start-up venture, it also has to deal with the risks of early exposure and negative feedback from the marketplace (DeSue, 2017 September 5; Reddit, 2017) until it demonstrates a solid track record of successful organizational level deployments and performance.

Lessons Learned: MEDRec

The MEDRec blockchain network is different from Patientory in that it was not initially designed to be a B2B2C network. It appears to be a more appropriate private permissioned blockchain environment consisting of a set of open application program interfaces (APIs) for a network of healthcare institutions that intend to collaborate to promote electronic health record review and exchange. MEDRec is a layer that can be added to the backends of existing provider IT systems through the use of the database gatekeeper utility (Ekblaw, 2017).

There are lessons to be learned from the limitations of the MEDRec 1.0 version. By design, patient data is not stored on the blockchain network. MEDRec uses pointers to direct queries to the provider databases that contain the relevant patient data that is being requested. This means MEDRec has no direct control over the security of the individual provider databases that participate in the MEDRec network. MEDRec, therefore, is totally dependent on the quality of security measures used

ISSN: 1941-6679-On-line Copy

by the IT staff of the provider organization. Also, MEDRec does not take responsibility for end-point security incidents which may involve situations where data vulnerability arises due to a compromised patient laptop or mobile device (Ekblaw, 2017). MEDRec also does not take prior responsibility for the digitization of medical records, which it assumes the provider IT infrastructure takes care of.

In conducting pilot tests of MEDRec with Beth Israel Deaconess Medical Center, the blockchain project team did not obtain a formal security review of the blockchain network's codebase, thus, it is highly possible for security vulnerabilities to exist, specifically in the structure of smart contracts (Ekblaw, 2017). The team, therefore, strongly recommend two important things: that a trained systems architect and security consultant highly familiar with blockchain conduct this security review of the codebase, and that encryption be used when the MEDRec blockchain network syncs with off-blockchain data that rests in provider databases to avert unauthorized content access.

There are also lessons to be learned and issues to be anticipated with regards to the scalability of the MEDRec network. Once the MEDRec network goes "live," thousands of databases could theoretically participate in its use. The first challenge is finding a way of keeping track of these participating databases and ensuring that they are, in fact, already networked and have previously authorized MEDRec's access to them (Ekblaw, 2017). MEDRec uses "smart contracts" that need to associate pointers to network locations of patient records where the database gatekeeper would need to retrieve data to satisfy queries. MEDRec faces the challenge of supporting a separate authentication scheme that enables the blockchain network to support both authentication and data connectivity among disparate databases supporting EHRs and health organizations, without having to use a central repository for authentication information (Ekblaw, 2017).

Another challenge involves being able to correctly associate the data for Patient X from hospital A with another set of data for the same Patient X from hospital B (Ekblaw, 2017). A serious issue that involves the entire healthcare industry is the mismatching patient records when retrieved from multiple healthcare organizations. Since electronic health record data exchange is central to MEDRec, ensuring correct patient matching of health records is essential. The reality is, though, failure rates for correctly matching patient records go as high as 50 percent (The Pew Charitable Trusts, 2018, October). By design, MEDRec does not attempt to resolve patient record mismatches.

ISSN: 1941-6679-On-line Copy

An issue related to patient matching of health records is the existence of significant volumes of the same patient health information using different record identifiers that are not linked

(Bell et al., 2018, July 9). Blockchain network performance degrades as the unnecessary duplication of patient records increases in frequency, also requiring the reduplication of records to allow the system to function using unique, anonymized identifiers to identify patients across all services.

Another challenge has to do with anticipating peak demand in the use of MEDRec especially on account of its medical research mining scheme, where many nodes would be pinging health provider databases with query requests from successfully mined blocks. The database servers of those providers would understandably be overloaded. Perhaps, to mitigate the problems that could result from this occurring, MEDRec could be redesigned to limit the number of whitelisted miners or the frequency at which they could retrieve their query results so as not to sacrifice the blockchain network performance or overload provider database networks.

Other challenges are relevant to the cost of the IT infrastructure required to be a participant in the MEDRec blockchain network. For instance, a healthcare provider can participate in the MEDRec network only if it invests in a software program that grants access to their internal databases while observing the rules of the MEDRec contract (Lippman et al., 2018, July). The monetary investment in this interfacing software program could be hefty, especially from the point of view of smaller healthcare providers.

MEDRec will continue to solicit the participation and interest of relevant healthcare organizations: care providers, hospitals, pharmaceutical firms, insurance firms, U.S. government bodies, healthcare startups, etc. (Ekblaw, 2017). MEDRec will also formalize the onboarding procedure for medical research miners, and conduct more user studies to assess patient, provider, and healthcare organization interest (Azaria et al., 2016). MEDRec based its functional requirements on information gathered in 2016 from use case scenarios obtained from the Kaiser Permanente, Beth Israel Deaconess Medical Center, Merck & Co., Department of Veterans Affairs, and others. Yet, the design team intends to improve the system even further by pursuing any of the following routes: (1) watching current developments in the evolution of blockchain technologies and go with a more stable version of Ethereum or a side-chain technology like the Lightning Network that will enable the design team to re-architect MEDRec on Bitcoin's scripting language "without bloating the Bitcoin blockchain…." (Ekblaw, 2017, p. 80); (2) pursue integration with the Hyperledger blockchain consortium; (3) learn from the current collaboration among

ISSN: 1941-6679-On-line Copy

Hyperledger, IBM, and WalMart in using blockchain for food provenance (Ekblaw, 2017); and (4) sustain commitment to the principles of open source software development in future MEDRec improvements (Halamka et al., 2017).

Both Patientory and MEDRec will be faced with certain similar hurdles as they head into the future. First of all, existing EHR systems are deeply entrenched in its existing architectures, are very conservative, and will not "jump" into the blockchain bandwagon easily (Drew, 2016, August). Seeking EHR adoption alone has been quite an obstacle and the Centers for Medicare and Medicaid Services (CMS) invested up to about US$30 billion in setting up EHR systems based on traditional technologies and architectures since 2014. This level of investment will not be abandoned readily despite the advantages of blockchain. To maintain a blockchain network infrastructure, an organizational stakeholder has to commit computing resources and a large number of independent nodes to conduct mining activities. Meanwhile, the computer infrastructures of existing hospital and healthcare organizations usually have a small number of nodes in their respective networks.

A more realistic approach would be to introduce a "bridge" solution that will work alongside existing EHR systems to provide an incremental transition to blockchain (Drew, 2016, August). Copies of healthcare data from traditional systems, using existing standards and policies, would be sent to the new blockchain based system such as the way MEDRec operates. Another possibility for a "bridge" solution is to use the blockchain as a service offerings of Patientory, which would provide most of the IT infrastructure components of blockchain for the network to function well.

Lessons Learned: Amerisourcebergen/Merck

One key lesson from the AmerisourceBergen/Merck experience is understanding how firms in the healthcare industry supply chain have to manage when certain government regulations are in play. AmerisourceBergen/Merck collaborated on the use of a blockchain network to meet the requirements of the Drug Quality and Security Act (DQSA) passed by U.S. Congress on November 27, 2013 and enforced by the Food and Drug Administration (FDA) (U.S. Food and Drug Administration, 2018). Title II of DQSA called the Drug Supply Chain Security Act (DSCSA) stipulates the steps in creating an electronic and interoperable system for identifying and tracing certain prescription drugs distributed in the U.S. This system is designed to protect consumers from counterfeit, stolen, contaminated, and harmful pharmaceutical products by assisting in detecting and removing dangerous drugs from the pharmaceutical supply chains in the U.S.

ISSN: 1941-6679-On-line Copy

The U.S. is the only country in the world that does not store pharmaceutical product information in a centralized database that can be accessed by all pharmaceutical supply chain members. In the U.S., drug manufacturers are expected to create their own numbering systems for their products and then, pass it on downstream to their trading partners like distributors/wholesalers and pharmacies. This has resulted in the existence of a wide range of product numbering systems that do not link with each other. In time, the U.S. realized the problems created by this system and thus, mandated what is called "serialization" of drug products in order to identify unique drug product units throughout the supply chain.

"Serialization" is a system of designating a unique serial number to each pharmaceutical product that is sold which links it to its origin, batch number, and expiration date (Wellspring Manufacturing Solutions, 2018). The serial numbers generated can be used to track individual drug products throughout its journey in the entire supply chain. The DQSA requires that drug products be serialized at both the item and case levels by November 2017. Drug manufacturers were not able to meet this deadline; the FDA granted an extension and also expressed that manufacturers should serialize their products even though they are not required to share product data downstream until 2023 (Denton, 2018).

AmerisourceBergen experienced challenges with respect to product returns from downstream customers such as clinics, hospitals, pharmacies, etc. Because of the 2023 final deadline for sharing drug product information downstream from the manufacturers, AmerisourceBergen, a distributor/wholesaler, does not have all serialized product information to help it determine if product returns from its customers are authentic or counterfeit products. Currently, it uses a tedious manual process involving making phone calls to drug manufacturers whose products are returned from customers (Denton, 2018). In the meantime also, AmerisourceBergen is accumulating returned products that are not properly processed and vetted that can easily cost the firm $3 billion a year. This is where the need for the blockchain network comes in. In addition to complying with the DSCSA requirements, AmerisourceBergen needed a better way to deal with its product returns before re-issuing returned drug products for sale again (Denton, 2018).

With respect to participating in blockchain networks with its trading partners, AmerisourceBergen expressed concern about future issues very likely to arise --- this is the second set of lessons. Jeff Denton, Senior Director of Global Secure Supply Chain for AmerisourceBergen, posed the following questions: how many blockchain networks does AmerisourceBergen have to participate in, in the near

ISSN: 1941-6679-On-line Copy

future --- drug manufacturers are very likely to set up their own networks. AmerisourceBergen as a distributor has to satisfy the needs of its manufacturer/customers. How will these multiple networks work together? How about governance --- how will multiple blockchain networks in the pharmaceutical industry be governed? There will also be third party blockchain network as a service providers who may be part of this ecosystem --- what is their role in this industry? (Denton, 2018). Denton also anticipates serious change management issues --- some colleagues may resist significant business process changes that the blockchain network will certainly require.

The third set of lessons have to do with how the blockchain network integrates with a firm's enterprisewide systems. First of all, AmerisourceBergen did the right thing when it integrated its blockchain network with its existing enterprise system using SAP's Advanced Track and Trace application. Director of IBM Blockchain Labs Nitin recommends carefully integrating a blockchain application with a firm's existing enterprise system in order to create a path with minimum disruption to the firm's business operations, while at the same time, facilitating enterprisewide adoption (Mougayar & Buterin, 2016). Also, creating a private blockchain that would serve the needs of AmerisourceBergen/Merck was the better way to go, rather than join a public blockchain network supported by a third party company.

The fourth set of lessons involve miscellaneous scalability and network expansion issues. It appears that AmerisourceBergen will store all its enterprise system data within their internal databases. The deployment of the CryptoWerks blockchain feature, however, will surely lead to the generation of larger volumes of data. AmerisourceBergen, therefore, should plan for this eventuality and its enterprise system should be able to manage the increased data storage and transaction handling. Should AmerisourceBergen consider the external data storage option as well, the firm needs to assess the potential third party provider, most likely a cloud service provider that enables cloud-based data storage, and ensure that layers of security and encryption technologies are used to protect its data (Morabito, 2017).

There are also other unique interorganizational adoption issues in the pharmaceutical industry supply chain (Shanley, 2017, August 1). A situation where, say, a distributor does business with many pharmaceutical manufacturing firms might call for subscription in a public blockchain network. This will allow the distributor to participate in multiple blockchains. However, adoption by small- and medium-sized distributors is unlikely since they would not have the financial means to do so. The same thing is true for serialization --- small- and medium-sized manufacturers and distributors are more likely to find the costs associated with serialization prohibitive. Then, there is the issue of the low levels of trust, if

ISSN: 1941-6679-On-line Copy

not total lack of it, between pharmaceutical manufacturers and distributors. This will surely discourage the conduct of blockchain proof-of-concept projects. When it comes to data collection, also, it is usually the distributors who make more money from collecting supply chain data (Shanley, 2017, August 1).

General Lessons

The following are "general lessons" that would apply to blockchain deployments of a wider range of healthcare organizations. Technical challenges that need to be addressed include (Zhang et al., 2018, March 1): ability to address the evolving the blockchain system; data storage; privacy; scalability; interoperability; and architecture.

Evolving the blockchain system involves the use of loosely coupled data structures that can accommodate needed changes without negatively impacting the ability of clients to interact with the data in the blockchain network. Also, healthcare data should be accessible from multiple healthcare systems that cannot be easily changed over the long term.

The **data storage challenge** is significant. Enormous volumes of data is expected to be stored with the participation of thousands if not millions of patients, care providers, billing agents, etc., and a variety of healthcare organizations. The data storage requirements will be even greater especially of data normalization and denormalization methods are not followed. If data storage requirements are not properly met, data access operations may be affected or may altogether fail especially if the blockchain network data size limit is exceeded. (Zhang et al., 2018, March 1).

The **privacy challenge** encompasses a number of concerns (Zhang et al., 2018, March 1). Regulatory agencies such as the US Office of the National Coordination for Health Information Technology (ONC) requires the following: (1) that participants in healthcare systems be properly identified and authenticated; (2) provide for a secure and ubiquitous IT infrastructure for data storage and exchange; (3) access controls and authorization procedures for different sources of external data; (4) manage the structures of a variety of data sources. Fortunately, the blockchain's inherent design principles involving the use of secure cryptography and support for robust peer-to-peer networks should address most of these requirements. On the other hand, an important risk in the blockchain network is the possibility of incidents of malfeasance involving the unforeseen unauthorized decrypting of private patient information on the blockchain.

ISSN: 1941-6679-On-line Copy

Related to the privacy challenge is the design decision involving the data to be stored in and off the blockchain network (Ribitzky et al., 2018). In this regard, it is prudent to follow the principle of data minimization involving both a "minimal and sufficient approach" in seeking to control data storage requirements and honoring privacy objectives in the network. Storing all accessible sensitive healthcare patient data on the network may not be wise, especially, if there is no clear reason for keeping and using the data upfront.

The **scalability challenge** involves the ability to anticipate and process a growing number of transactions as patients' healthcare needs change and as the growing number of patients in each healthcare system interacts with different stakeholders --- care providers, hospitals, specialist private clinics, regional urgent care centers, insurance companies, etc. Scalability should allow for providing activity monitoring and filtering, both of which would demand considerable compute power in order to track and report patient health status reliably (Zhang et al., 2018, March 1).

Interoperability means that the blockchain network will be able to work with other EHR and CMR systems and exchange data/information. Interoperability is enabled by defining the data structure, semantic integrity, reference terminologies, code sets employed, and status of stored data (Ribitzky et al., 2018). Pointers to off-chain data and their associated metadata support interoperability. Related to interoperability, the blockchain network can allow maximum availability and security through the use of smart contracts and the extension of vertical service-level healthcare interoperability application programming interface (API) patterns to serve data transactions in the blockchain network.

Finally, another challenge involves the choice of the **blockchain deployment architecture**. The choices are: public versus private and permissioned versus permissionless environments. Each alternative has its own implications in terms of resources needed for privacy, security, compliance, operational performance, deployment, and ongoing operational/maintenance. Public blockchains would be appropriate in situations where nonsensitive information is being exchanged. This is more likely not the case with sensitive patient healthcare information --- thus, private and permissioned blockchains are the better choice here. To protect the network's security, data encryption and the use of the principle of least privilege is best applied ensuring that participants accessing the network have the permissions to do so.

The main contributions of this paper are the following. First, this descriptive study constitutes more of a "general review" paper that provides an overview of a newly

developing information technology and how it is currently emerging in the marketplace. The healthcare system in North America is beset with major challenges preventing it from being truly of service to society. It behooves technology experts to apply tools that address pressing healthcare industry problems that include data interoperability among electronic health record (EHR) systems, insurance claim notarization and payments, billing, drug supply chain provenance, cybersecurity, patient privacy, government regulation compliance, etc. (Frost & Sullivan, (2017, September 5). Second, data for use cases that were most evident and available for analysis and study by academic researchers are presented in this descriptive study. Third, the author extends the description of these three proof-of-concept cases by drilling down into the lessons learned and challenges the organizations face moving forward.

REFERENCES

Antonovici, A. (2018, June 8). AmerisourceBergen, Merck to Expand Blockchain Test Project for Tracking Drugs. Crypto Vest website. Retrieved from https://cryptovest.com/news/amerisourcebergen-merck-to-expand-blockchain-test-project-for-tracking-drugs/

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. Proceedings of the IEEE 2016 2nd International Conference on Open and Big Data. August 22-24. Vienna, Austria.

Becker's Health IT & CIO Report (2017, January 19). How Patientory uses blockchain to keep data secure and help connect patients. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/how-patientory-uses-blockchain-to-keep-data-secure-and-help-connect-patients.html

Bell, L., Buchanan, W.J., Cameron, J. and Lo, O. (2018, July 9). Applications of Blockchain Within Healthcare. Blockchain in Healthcare Today website. Retrieved from https://blockchainhealthcaretoday.com/index.php/journal/article/view/8/40

Bitcoin Magazine (n.d.). Patientory's Journey to Change Healthcare. Retrieved from https://bitcoinmagazine.com/articles/patientorys-journey-change-healthcare/

ISSN: 1941-6679-On-line Copy

Bylo, G. (2017, April 7). Bracing for Drug Tracing Mandate. PharmExec.com website. Retrieved from http://www.pharmexec.com/bracing-drug-tracing-mandate

Chatterjee, B. (2015, January 20). Serialization and the Drug Quality & Security Act. Pharmaceutical Manufacturing website. Retrieved from https://www.pharmamanufacturing.com/articles/2015/serialization-drug-quality-security-act/

Cohen, J.K. (2017, August 31). Patientory, Oracle join Hyperledger blockchain effort. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/patientory-oracle-join-hyperledger-blockchain-effort.html

CryptoWerk (2018a). Enterprise Blockchain FAQs. Retrieved from https://gn680kq70q1w32f915vk8a75-wpengine.netdna-ssl.com/wp-content/uploads/2018/03/CryptowerkFAQs.pdf

CryptoWerk (2018b). Blockchain Enablement Kit. Retrieved from https://cryptowerk.com/blockchain-enablement-kit-white-paper/

CryptoWerk (2018c). Case Study: Pharma: Pharma Leaders Partner with SAP and CryptoWerk on Blockchain-Powered POC. Retrieved from https://gn680kq70q1w32f915vk8a75-wpengine.netdna-ssl.com/wp-content/uploads/2018/01/PharmaCaseStudy.pdf

CryptoWerk (2018d). Merck and Amerisourcebergen Partner with CryptoWerk and SAP to Explore the Benefits of Blockchain for Supply Chain Applications. Paul Cocuzzo, Director of Supply Chain, Merck and Company, Inc. [Video transcript]. Retrieved from https://cryptowerk.com/pharma-leaders-embrace-blockchain/

CryptoWerk (2018e). Merck and Amerisourcebergen Partner with CryptoWerk and SAP to Explore the Benefits of Blockchain for Supply Chain Applications. Jeff Denton, Sr. Director, Global Secure Supply Chain, Amerisource Bergen. [Video transcript]. Retrieved from https://cryptowerk.com/pharma-leaders-embrace-blockchain/

Denton, J. (2018). Blockchain Solutions to Meet FDA Drug Supply Chain Security Act, Jeff Denton, AmerisourceBergen. Talk Sponsored by the

ARC Advisory Group. Jeff Denton, Senior Director, Global Secure Supply Chain, AmerisourceBergen. [Video transcript]. Retrieved from https://www.youtube.com/watch?v=puTf-xN4brk

DeSue, T. (2017, September 5). Patientory's Poor PR Skills Overshadow ICO. Cryptovest website. Retrieved from https://cryptovest.com/features/patientorys-poor-pr-skills-overshadow-ico/

Drew, I. (2016, August). Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. Retrieved from https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf

Ekblaw, A. (2017). MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis (Masteral thesis). Retrieved from https://dspace.mit.edu/handle/1721.1/109658

Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. Whitepaper. August. Retrieved from https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

Frost & Sullivan (2018, April 18). Top Trends and Outlook in Health IT: HIMSS 2018 Conference Report by Nancy Fabozzi. Retrieved from Frost & Sullivan database (restricted access).

Frost & Sullivan (2018, January). Global Healthcare Industry Outlook, 2018. Retrieved from Frost & Sullivan database (restricted access).

Frost & Sullivan (2017, September 5). Top 5 Reasons Why Every Healthcare Company Should Invest in Blockchain. . Retrieved from Frost & Sullivan database (restricted access).

Frost & Sullivan (2017, August 4). Why Healthcare Industry Should Care About Blockchain. Retrieved from Frost & Sullivan database (restricted access).

Frost & Sullivan (2017, June). Blockchain Technology in Global Healthcare, 2017-2025. Retrieved from Frost & Sullivan database (restricted access).

ISSN: 1941-6679-On-line Copy

Frost & Sullivan (2016, November). Vision 2025: The Future of Healthcare. Retrieved from Frost & Sullivan database (restricted access).

Gaskell, A. (2017, May 3). The Move Towards Healthcare Blockchains. Retrieved from https://www.huffingtonpost.com/entry/the-move-towards-healthcare-blockchains_us_59003a9be4b06feec8ac91e1

Gupta, V. (2017). A Brief History of Blockchain. *Harvard Business Review Digital Articles*, February 28, 2-4.

Halamka, J.D., Lippman, A., & Ekblaw, A. (2017). The Potential for Blockchain to Transform Electronic Health Records. *Harvard Business Review Digital Articles*, March 3, 2-5.

Health Transformer (2017, August 29). Patientory Takes Another Big Step Towards Interoperability. Retrieved from https://healthtransformer.co/patientory-takes-another-big-step-towards-interoperability-2d1741d39ca

Hecker, B. (2018, June 15). Bernhard Hecker, Cryptowerk --- NOAH18 Berlin. Bernhard Hecker, CEO, CryptoWerk. [Video transcript]. Retrieved from https://www.youtube.com/watch?v=ICW-ThgbaCM&t=10s

Iansiti, M., & Lakhani, K.R. (2017). The Truth About Blockchain. *Harvard Business Review*, 95 (1), 118-127.

Lippman, A., Nchinda, N., Retzepi, K. and Cameron, A. (2018, July). MedRec: Patient Control of Medical Record Distribution. *IEEE Blockchain Newsletter*. Retrieved from https://blockchain.ieee.org/newsletter/july-2018/medRec-patient-control-of-medical-record-distribution

Mainelli, M. (2017). Blockchain Could Help Us Reclaim Control of Our Personal Data. *Harvard Business Review Digital Articles*, October 5, 2-5.

Marr, B. (2018, January 25). Why The Internet of Medical Things (IoMT) Will Start to Transform Healthcare In 2018. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#67d222034a3c

McFarlane, C., Beer, M., Brown, J., & Prendergast, N. (2017). Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1, Whitepaper. May. Retrieved from https://patientory.com/patientory_whitepaper.pdf

McKesson Ventures (2017, May 10). How Blockchain Could Rebuild the Healthcare Industry. McKesson Ventures website. Retrieved from http://ventures.mckesson.com/blockchain-rebuild-healthcare-industry/

Morabito, V. (2017). Business Innovation Through Blockchain: The B3 Perspective. New York, NY: Springer.

Mougayar, W. and Buterin, V. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken, NJ: John Wiley & Sons.

Patientory (2018, September 23). Pharma Intelligence Congratulates Winners of the Inaugural MedTech Insight Awards [Including Patientory CEO Chrissa McFarlane]. Patientory Blog. Retrieved from https://patientory.com/blog/2018/10/16/pharma-intelligence-congratulates-winners-of-the-inaugural-medtech-insight-awards-including-patientory-ceo-chrissa-mcfarlane/

Patientory (2018, August 28). Innovation to Transformation: Forging the Path to Consumer-directed Health, Distributed App Version 1. Beta User Survey Results. Retrieved from https://patientory.com/wp-content/uploads/2017/04/patientory-dapp-user-survey-results-2018.pdf

Patientory (2018, March 1). The Patientory Stiftung Makeover. Patientory Blog. Retrieved from https://patientory.com/blog/2018/03/01/patientory-stiftung-makeover/

Patientory (2017, November 7). Blockchain-Healthcare Start-Up Patientory Wins Two Prestigious Awards. Patientory Blog. Retrieved from https://patientory.com/blog/2017/11/07/blockchain-healthcare-start-patientory-wins-two-prestigious-awards/

Patientory (2017, August 29). Patientory Joins Forces With Hyperledger. Patientory Blog. Retrieved from https://patientory.com/blog/2017/08/29/patientory-joins-forces-hyperledger/

ISSN: 1941-6679-On-line Copy

Patientory (2017a, June 20). Patientory Live Update and AMA #1. [Video transcript]. Retrieved from https://patientory.com/videos/

Patientory (2017b, July 24). Patientory Live Update and AMA #1. [Video transcript]. Retrieved from https://patientory.com/videos/

Patientory (2017, June 3). Patientory Raises $7.2 Million USD to Transform Healthcare. Patientory Blog. Retrieved from https://patientory.com/blog/2017/06/04/patientory-raises-7-2-million-usd-transform-healthcare/

Patientory (2017, May 3). Patientory Wins Top Price At SEMDA 2017 to Transform Healthcare Using Blockchain. Patientory Blog. Retrieved from https://patientory.com/blog/2017/05/03/patientory-wins-top-prize-semda2017-transform-healthcare-using-blockchain/

Patientory (no date n.d.a). Patientory to Integrate Dash Payments Using BlockCypher Web Services. Patientory Blog. Retrieved from https://patientory.com/blog/2017/08/24/patientory-integrate-dash-payments-using-blockcypher-web-services/

Reddit (2017). Beware of PTOY (Patientory). Reddit Blog. Retrieved from https://www.reddit.com/r/CryptoCurrency/comments/70e9h7/beware_of_ptoy_patientory/

Ribitzky, R., St. Clair, J., Houlding, D.I., McFarlane, C.T., Ahier, B., Gould, M., Flannery, H.L., Pupo, E., & Clauson, K.A. (2018). Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare. Blockchain in Healthcare Today. Volume 1, March 23. Retrieved from https://blockchainhealthcaretoday.com/index.php/journal/article/view/24

SAP (2018, April 6). SAP Advanced Track and Trace for Pharmaceuticals. Retrieved from https://www.sap.com/canada/products/pharmaceutical-track-trace.html

Shanley, A. (2017, August 1). Could Blockchain Improve Pharmaceutical Supply Chain Security? Pharmaceutical Technology website. Retrieved from http://www.pharmtech.com/could-blockchain-improve-pharmaceutical-supply-chain-security

ISSN: 1941-6679-On-line Copy

The Medical Futurist (2018, March 27). Top 12 Companies Bringing Blockchain To Healthcare. The Medical Futurist website. Retrieved from https://medicalfuturist.com/top-12-companies-bringing-blockchain-to-healthcare

The Pew Charitable Trusts (2018, October). A Report from The Pew Charitable Trusts: Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records. Retrieved from https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records

U.S. Food and Drug Administration (2018). Drug Supply Chain Security Act (DSCSA). Retrieved from https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/#top

Wellspring Manufacturing Solutions (2018). Serialization: What it means for pharmaceutical manufacturing. Wellspring Manufacturing Solutions website. Retrieved from http://www.wellspringcmo.com/blog/serialization-what-it-means-for-pharmaceutical-manufacturing

Zhang, P., Schmidt, D.C., & White, J. (2018, March 1). Book Chapter Proposal: Chapter 3: Blockchain Technology Use Cases in Healthcare. Retrieved from http://www.dre.vanderbilt.edu/~schmidt/PDF/blockchain-bookchapter-2018.pdf

ISSN: 1941-6679-On-line Copy