Lex Mundi Blockchain White Paper Series

Transforming the U.S. Healthcare Industry with Blockchain Technology

by F. Dario de Martino, Spencer D. Klein, Julie O'Neil, Yiyang Huang, Lee Nisson and Mary Race
Morrison & Foerster LLP (Lex Mundi member firm for USA, California)

Patients accumulate vast quantities of healthcare data over the course of their lives. Those data are generally housed in centralized servers operated by various unrelated industry participants, including government regulators and payors, insurance carriers, hospitals, doctors, pharmacies and pharmaceutical companies.

Unfortunately, those repositories rely on disparate data practices. In addition, they are alluring targets for bad actors. In October 2009, the U.S. Department of Health and Human Services' Office for Civil Rights (DOH) began publishing statistics for data breaches involving U.S. healthcare information.[1] What began as a low rumble in 2009 has crested into a wave of leaked information nearly a decade later. For example, in 2015, more than 100 million Americans had their healthcare data taken without their permission.[2] Though 2015 was an outlier in terms of the sheer volume of information taken, the picture painted by the DOH's statistics indicates that since the agency began reporting, more than half of the entire population of the United States has had their medical records compromised.[3] Cries of recrimination, class action lawsuits, self-reflection, and calls for, and the passage of, robust regulation shortly followed.

Nevertheless, while the industry has made a concerted effort to get ahead of the problem, healthcare data stolen from intermediary servers remains fairly commonplace. The consequence is that many healthcare organizations are in the crosshairs of patients, regulators and consumer protection advocates alike, and the costs of failure are mounting.

Fortuitously, as for many other issues facing the healthcare industry, blockchain technology offers a potential solution.

[1] *See* Healthcare Breach Statistics, HIPAA Journal, *available at:* https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[2] *See* U.S. Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, *available at:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf; and Thomas H. McCoy, Roy H. Perlis, *Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017*, Journal of the American Medical Association (Sept. 25, 2018), *available at:* https://jamanetwork.com/journals/jama/article-abstract/2703327.
[3] *See supra* note 1.

Blockchain and Smart Contracts Defined

At its core, a blockchain is a data structure that makes it possible to create a tamper-proof, distributed, peer-to-peer system of ledgers containing immutable, time-stamped, and cryptographically connected blocks of data. In practice this means that data can be written only once onto a ledger which is then read-only for every user. Many of the well-known applications of blockchain technology, such as Bitcoin and Ethereum, maintain and update these distributed ledgers in a decentralized manner. Crucially, these mechanisms function to remove the need for a trusted third party to handle and store the transaction data and instead distribute the data so that every user has access to the same information at the same time. In order to update that ledger's distributed information, the networks employ pre-defined consensus mechanisms and military-grade cryptography to prevent malicious actors from going back and retroactively editing or tampering with the information previously recorded on it. In most cases, the networks are open-source, maintained by a dedicated community, and made accessible to any connected device that can validate transactions on the ledger, which is referred to as a node.

Nevertheless, the decentralizing feature of blockchain comes with significant resource and processing drawbacks. Many blockchain-enabled platforms run very slowly and have infamous scalability problems. Moreover, these networks use massive amounts of energy. For example, the Bitcoin network's consensus mechanisms require the expenditure of about 50 terawatt hours per year –equivalent to the energy needs of the entire country of Singapore.[4] To ameliorate these problems, several industry participants have developed enterprise blockchains with permissioned networks. While they may be open-source, the networks are led by known entities that determine who may verify transactions on that blockchain, and therefore the required consensus mechanisms are much more energy efficient.

Although blockchain is a ground-breaking technology, it needed several improvements to become a candidate for wider application. And a wide-spread application of the technology arguably started with the introduction of Ethereum and "smart contracts" - a term used to describe computer code that automatically executes all or part of an agreement and is stored on a blockchain-enabled platform. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those coded parameters. The input parameters and the execution steps for smart contracts need to be specific – the digital equivalent of an if "x", then "y" statement. In other words, when the required conditions have been met, such as delivery of a product, a particular specified outcome would occur, such as the making of a payment; in the same way that a vending machine sells a can of soda once change has been deposited, smart contracts allow title to digital assets to move upon the occurrence of certain events. However, the tasks that smart contracts are performing are currently fairly rudimentary. As the adoption of blockchain spreads, we believe smart contracts will likely become increasingly complex, especially when integrated with other technologies such as artificial intelligence (AI), where blockchain delivers trusted and immutable data for AI, and AI delivers cognition and automation to business processes. Therefore, we believe blockchain and smart contracts will be capable of handling sophisticated transactions and will facilitate the creation of a more synchronized and integrated healthcare ecosystem.

The Healthcare Industry and Blockchain's Potential

Healthcare is becoming increasingly expensive. According to the Centers for Medicare & Medicaid Services (CMS), U.S. healthcare spending reached $3.5 trillion (or $10,739 per capita) in 2017, representing a 17.9% share of the U.S. GDP.[5] That number is projected by CMS to reach nearly $5.5 trillion by 2025, mainly fueled

[4] *See* Bitcoin Energy Consumption Index (last accessed Sept. 21, 2018), *available at:* https://digiconomist.net/bitcoin-energy-consumption.
[5] National Health Expenditures 2017 Highlights, Centers for Medicare & Medicaid Services, *available at:* https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/highlights.pdf.

by an aging population and rising prices for healthcare services, generating a growth rate outpacing that of America's economy as a whole by 1.2 percentage points.[6]

Blockchain, with its ability to improve data security, synchronize vast quantities of data and ensure transaction integrity among a variety of industry participants could have important applications in this large and growing industry in which security is paramount. In addition, smart contracts can increase transactional efficiency, and in that process provide more efficient health care and increase the bottom line for pharmaceutical development activities.

However, blockchain technology is no panacea for the many problems facing the healthcare industry. After some initial exploration, and as the sector matured, industry participants have been able to separate the wheat from the chaff, and as a result several real-world use cases have emerged as strong candidates for a blockchain-based solution. While approaches highlighted in the following paragraphs are certainly not the only use cases where this technology may be effective, they provide significant examples of challenges that may be best surmounted with blockchain technology. As such, with careful coordination among legal counsel, technologists, executives and consumer advocates, blockchain technology could be a major boon to the healthcare industry.

Counterfeit Pharmaceuticals

Drug counterfeiting is a well-documented problem in the pharmaceutical industry. The Health Research Funding Organization estimates that 10% of the drugs sold in developing countries are counterfeit with statistics reaching as high as 10% to 30% in Asia, Africa and Latin America.[7] According to the World Health Organization, counterfeit drugs often contain the wrong ingredients or wrong levels of key ingredients, rendering them ineffective at best and potentially lethal at worst.[8] Counterfeit drugs also harm the return on investment of pharmaceutical companies.[9] The main problem stems from a lack of transparency in the supply chain for drugs – without effective data sharing, there are no complete and traceable records across the supply chain. This creates several points of potential failure from ingredients sourcing, drug manufacturing, distribution processes and final product authentication.

In the United States, to ameliorate this issue and protect consumers from counterfeit drugs, Congress passed the Drug Supply Chain Security Act (DSCSA) in 2013. The DSCSA requires drug manufacturers of pharmaceutical products sold in the United States to serialize, or uniquely identify, pharmaceutical products. Importantly DSCSA also requires that all supply chain participants share certain information for interoperable, electronic tracing of prescription drugs over a 10-year period, with an implementation deadline for traceability on November 27, 2023.[10]

Blockchain offers a promising solution to enable pharmaceutical traceability, real-time access to data and supply chain validation by creating a log to track each step of the supply chain, and some promising projects are making progress in this area.

The MediLedger Project started in 2017 to explore if blockchain could provide solutions for DSCSA compliance. One solution, the MediLedger Look-Up Directory, utilizes a messaging network underpinned by a permissioned

---

[6] *See CMS: US healthcare spending to reach nearly 20% of GDP by 2025* (Feb. 16, 2017), *available at:* https://www.advisory.com/daily-briefing/2017/02/16/spending-growth.

[7] United Nations Office on Drugs and Crime, *Counterfeit Goods: A Bargain or A Costly Mistake?* (accessed Jan. 23, 2019), *available at:* www.unodc.org/toc/en/crimes/counterfeit-goods.html.

[8] *See* Substandard and Falsified Medical Products (accessed Jan. 24, 2019), World Health Organization (Jan. 31, 2018), *available at:* https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

[9] *Id.*

[10] Title II of the Drug Quality and Security Act, The U.S Food and Drug Administration website (last updated Dec. 16, 2014), *available at:* http://www.fda.gov/drugs/drugsafety/drugintegrityandsupplychainsecurity/drugsupplychainsecurityact/ucm376829.htm.

blockchain system that allows companies to securely send and respond to product identifier verification requests. If the request clears, the pharmaceutical product can move forward along the supply chain without the additional need for cumbersome and expensive verification procedures, since the information contained on the blockchain is inherently trustworthy. Crucially, only authorized companies can key their products into the Look-Up Directory. Thus, the likelihood that bad actors are able to disguise their counterfeits as genuine pharmaceuticals is severely reduced. As of the time this article was written, the project has passed the test of concept stage and is testing additional functionalities with commercial launches planned for the near future.

It is also worth noting that IBM Research has spearheaded a research project in Haifa, Israel to track, trace and authenticate drugs at each stage of the drug supply chain in an effort to reduce or eliminate the severe drug counterfeiting problems in Kenya. The IBM project uses a mobile interface and a permissioned blockchain that enables each certified and authorized party in the network to track its transactions through a jointly verifiable ledger.[11] Once a party has been vetted by the project as a trustworthy supplier or service, the project's blockchain-dependent QR codes act as the keystone for the remaining links in the supply chain. Each drug delivery along the way, from the pharmacy to the final recipient, is then rescanned, verified and tracked by a user-friendly mobile interface on top of the blockchain's ledger, thus encouraging the parties to trust that the medicine is indeed genuine.

These projects, among others tailored to supply chains across other industries, show the remarkable potential for blockchain to offer an effective solution for the counterfeit drug problem and DSCSA compliance. However, challenges remain, as the implementation of an infant technology like blockchain could be costly, especially in the short-term.

Clinical Data and Medical Record Interoperability

Patients tend to leave a large paper trail. They create medical records with various providers whenever they change healthcare plans, move to a new city or visit specialists. Unfortunately, these providers rarely communicate with one another, and the patient's records typically reside in separate data silos, each with a unique filing method, descriptive semantics and security mechanisms. All combined, the current system makes it difficult for patients, regulators, providers and payers to easily access and securely share data; moreover, physicians often lack comprehensive information to understand a patient's medical history and total health – thus reducing medical care quality and increasing the likelihood of additional costs with duplicate tests. In addition, as patients move from one healthcare provider to another, the data are retained by the old provider and duplicated as the new patient inputs information into the new provider's system. Given the varied levels of security among these many stakeholders, each with different or duplicated patient data, it is not surprising that more than half of the entire population of the United States has had their medical records compromised.[12]

With blockchain, healthcare data can be unified into one distributed ledger that can be more securely shared among providers, who would have access to the same information. A blockchain-enabled platform could allow providers to directly access and exchange the same set of healthcare records through a secured shared ledger. Furthermore, patients could retain control over granting and rescinding permission for providers to access their medical records. Patients would be empowered to take control of their encrypted records by choosing to upload them to a distributed blockchain network rather than leave them in the provider's care. This innovation could improve data flow, and remove the additional compliance headaches and costs of having to secure each patient's data on a provider's own system.

[11] See Using blockchain to prevent counterfeit drugs in Kenya, IBM Research (July 27, 2017), *available at:* https://www.youtube.com/watch?v=11Z4-XYoZAE&feature=youtu.be.

[12] *See supra* note 1.

Indeed, the timing for these developments could not be better. Cybersecurity and data privacy are increasingly coming to the forefront for industry participants. In addition, there are a number of regulations associated with providing and collecting personal data that must be taken into account when deploying blockchain technology in healthcare. Europe's General Data Protection Regulation (GDPR) has led the way, but comprehensive data protection laws applicable to the U.S. healthcare industry are already close to home, especially with California's recently enactment of the California Consumer Privacy Act (CCPA).[13] Though some of the specifics may change, at its core, the CCPA covers, but is not limited to, 11 different types of personal data, including the biometric variety.[14] Should a healthcare company fall under its purview, the compliance challenges could be significant. In addition, the CCPA gives California residents a right to sue in the cases where their data were breached as a result of a business's failure to implement and maintain "reasonable security procedures and practices" to protect it.[15] Nevertheless, healthcare data governed by the Health Insurance Portability and Accountability Act (HIPAA) is largely exempted from the CCPA, and the exemption was expanded upon by a recent amendment.[16] However, the amendment passed only after a hard-fought lobbying effort. Moreover, many healthcare experts handle patient data that may fall outside HIPAA's regulatory regime, potentially subjecting such data to the CCPA. As data privacy increasingly becomes in vogue, the cost of handling patient data in a less than robust way has the potential to create significant liability.

A number of blockchain projects are getting ahead of the problem and taking concrete steps to address the interoperability and security problems plaguing healthcare data systems. One such entity, PokitDok, a platform-based blockchain company, developed its own system for letting diverse stakeholders and patients access these conflicting healthcare record systems. Many of the communications between healthcare providers and consumers are protected by identity safeguards put in place by HIPAA. However PokitDok's DokChain system makes it so that once an identity is established that satisfies HIPAA, the network can securely facilitate transactions between patients and providers in a fraction of the time.[17] PokitDok is hardly the only player in this space. Among others, MedRec, led by the MIT Media Lab and Beth Israel Deaconess Medical Center, is another player that is rethinking data security in health care. MedRec fully decentralizes access rights to healthcare data via an Ethereum blockchain, thereby giving patients control over record distribution.[18]

Claims Processing and Smart Contracts

The current system for processing healthcare claims and reimbursement is riddled with inefficiencies and is prone to errors. Blockchain technology can dramatically reduce the friction of medical billing, making claims processing more efficient, transparent and less costly while vastly reducing the likelihood of potential fraud. Ultimately, blockchain's relevance to billing stems from its ability to offer a bedrock of truth that all parties can access and rely on.

Blockchain could enable insurers like Medicare to effortlessly pay claims once they are verified on the blockchain-enabled ledger and ignore fraudulent ones. The use of smart contracts could further streamline the claims process. A smart contract could empower a patient to automatically grant access to his or her healthcare record

[13] *See* California Consumer Privacy Act, State of California Department of Justice (last accessed Sept. 22, 2018), *available at:* https://oag.ca.gov/privacy/ccpa.
[14] Cal. Civ. Code 3 § 1798.140(o)(1).
[15] *Id.*, § 1798.150(a).
[16] *Id.*, § 1798.145(c).
[17] *See* Ron Miller, PokitDok Teams with Intel on Healthcare Blockchain Solution, TechCrunch (May 10, 2017), available at: https://techcrunch.com/2017/05/10/pokitdok-teams-with-intel-on-healthcare-blockchain-solution/.
[18] *See* Asaph Azaria, Ariel Ekblaw, John D. Halamka, and Andrew Lippman, *A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data* (Aug. 2016), *available at:* https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5a6fd2f7e2c48387dff12676/1517278000381/blockchain-medical-records-patient-data-medrec-eckblaw.pdf.

to a doctor or list of doctors or facilitate instantaneous claim processing of the underlying code upon submission of claims.

Exciting developments have been made in this area. On November 5, 2018, Change Healthcare and TIBCO Software announced a collaboration to build a smart contract system aimed at improving healthcare claim processes using Change Healthcare's blockchain technology and TIBCO's smart contract development project.[19] This platform will attempt to enable health plans and their partners to easily develop and use smart contract-based processes that automate steps in the healthcare transaction processing cycle in order to lower costs and speed up the claim resolution and payment remittance processes.[20]

Structuring smart contracts in a way to ensure enforceability will be key, and various legal issues will need to be addressed, including enforceability under electronic signature and contract laws, dispute resolution mechanisms and jurisdictional issues.

Clinical Trial Fraud and Reproducibility

Reproducible data is the lifeblood of advanced research across the globe. The fact that scientists are able to reproduce results from one experiment to another is what allows the community at large to have faith in a study's scientific conclusions, which thus empowers humanity as a whole to make progress. Unfortunately, the current methods for preserving and reproducing data from clinical trials are inadequate. A review of more than 2,000 articles about the results of clinical trials that were retracted by major journals revealed that more than two-thirds were retracted because of some type of fraud.[21]

These retractions come with serious consequences. In addition to the waste of running expensive medical trials that have no merit, medical decisions made by physicians and research scientists on the premise of fraudulent data could leave patients at risk. Some studies indicate that hundreds of thousands of patients have been affected by improper medical care caused by fraudulent studies or the administration of improper treatment based on fraudulent studies. The monetary cost is also staggering; by one estimate, every paper retracted because of research misconduct costs about $400,000 in funds from the U.S. National Institutes of Health (NIH).[22] And that is just one institution; a more alarming calculation places the cost at $28 billion per year for preclinical research that isn't reproducible.[23] The costs are not limited to past events. Forward-looking medical licensing arrangements are quick to lose their value if it is revealed that the clinical findings upon which they were predicated were duplicitous. Experienced attorneys may be able to contract around these mitigating circumstances, but the more likely outcome in such cases is costly and protracted litigation.

One of the great innovations of blockchain is that its distributed nature and use of cryptography make it so that records entered onto its ledger are not retroactively changeable. The opportunities to revise experiment results to fit a preconceived hypothesis are thus eliminated and every entry onto a blockchain is traceable. For a researcher looking to reproduce results gleaned from an experiment's data, being able to chart a predecessor's steps with full certainty of the path taken is particularly crucial. That isn't to say that a blockchain can make fraudulent data entered onto it any less fraudulent than it actually was in real life – garbage in does not make gospel out.

---

[19] *See Change Healthcare and TIBCO to Bring Blockchain-Powered Smart Contracts to Healthcare* (Nov. 5, 2018), *available at:* https://www.changehealthcare.com/press-room/press-releases/detail/change-healthcare-and-tibco-bring-blockchain-to-healthcare.

[20] *Id. supra* note 17.

[21] *See* David Randall, Christopher Welser, *The Irreproducibility Crisis of Modern Science*, National Association of Scholars (Apr. 26, 2018), *available at:* https://www.nas.org/images/documents/NAS_irreproducibilityReport.pdf.

[22] See Andrew M. Stern, Arturo Casadevall, R. Grant Steen, and Ferric C. Fang, *Financial Costs and Personal Consequences of Research Misconduct Resulting in Retracted Publications*, eLife (Aug. 14, 2014), *available at:* https://elifesciences.org/articles/02956.

[23] See Iain Cockburn, Leonard Freedman, and Timothy Simcoe, *The Economics of Reproducibility in Preclinical Research*, PLOS Biology (June 9, 2015), *available at:* https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.1002165.

One emerging company enabling an integrated ecosystem of validated information is MyIRE. The company has developed an all-in-one modular blockchain-enabled system that allows its stored information to be callable and traceable to varying degrees, depending on the stakeholder within the network, for every stage of an experiment's research lifecycle.[24] Researchers who upload their results onto MyIRE's platform are able to trace back their data and know it hasn't been tampered with. Likewise publishers, watchdogs and regulators can read information that has been uploaded to ascertain where it came from. Research fraud may be a systemic failure of the scientific community, but tools like the MyIRE platform may allow it to correct its course efficiently for society's benefit.

Conclusion

The application of blockchain to the healthcare industry is still in its infant stages and its widespread adoption faces many challenges, including its technical ability to scale, interoperability, potential resistance from existing stakeholders to navigate issues around standardized data practices, regulatory limitations, acceptance of enhanced levels of transparency, and competition from other emerging technologies.

However, we believe it truly is an exciting time for the healthcare industry to tap into the potential of blockchain technology and contribute to its development and widespread adoption.

For more information, contact bd@lexmundi.com.

[24] *See MYR – The Reproducible Research Token* (June 2018), *available at:* https://myire.com/public/static/downloads/MYR_The_Reproducible_Research_Token.pdf.