HealthManagement
Promoting Management and Leadership

Volume 17 - Issue 4, 2017 - Cover Story: Risk & Danger

Is blockchain technology the solution to healthcare's data woes?

Sharon Klein
******@***pepperlaw.com

Partner, Pepper Hamilton LL P
Philadelphia, USA

LinkedIn Twitter

Joseph Guagliardo
******@***pepperlaw.com

Partner, Pepper Hamilton LL P
Philadelphia, USA

LinkedIn

In healthcare, blockchain is widely regarded as technology that will protect data from costly and credibility-damaging cyberhacking. But there's a risk; does it align with regulatory bodies' criteria?

Many experts believe blockchain technology will drive innovation in health information and that it has the potential to solve critical healthcare issues, including interoperability, security, records management and data exchange. As with any new technology in a heavily regulated industry, widespread adoption of blockchain technology in healthcare is highly dependent on striking the right balance between innovation and regulation. Finding that balance requires an understanding of both the technology and the regulatory boundaries.

The fundamentals of blockchain technology

At a fundamental level, blockchain technology is distributed peer-to-peer ledger technology built around four key concepts: decentralised digital trust, consensus protocol, immutability and security. Generally, blockchain technology structures each transaction into chronologically recorded blocks of data that are encrypted on a distributed (public, semi-private or private) database (Linn and Koo 2016). Each hash in a blockchain database uses the new data to be recorded and old data from a previous block to create a unique and immutable digital signature for each new block of data (Linn and Koo 2016).

To verify that each subsequent block in a chain matches up with all previous blocks (and is otherwise a valid transaction), blockchain technology uses a form of consensus protocol to confirm transactions before they are written to the database (Linn and Koo 2016). Each member (or node) in a distributed blockchain network stores an identical copy of the entire database and participates in the collective verification process in real time by simultaneously running algorithms to confirm transactions (Economist 2016). Because each new block's hash is based on the hash of a previous block, any change to a past transaction is immediately apparent to everyone in the chain when the hash of a new block no longer matches up with the chain of blocks before it. At a basic level, this network consensus and transparency increases security and immutability of transactions that are written to the database and may replace a trusted intermediary (Linn and Koo 2016).

What are the challenges of implementing blockchain technology in healthcare?

One of healthcare's greatest challenges is interoperability and managing patient data across the continuum of care. Blockchain technology has the potential to solve this challenge, but experts still express some technological and regulatory concerns. Two challenges are scalability and privacy (IB M Global Business Services Public Sector Team 2016).

Blockchain technology is ideal for smaller data units, but the size of medical records would quickly make scalability problematic if applied to a traditional blockchain structure (Linn and Koo 2016). Complete medical records of each patient in a blockchain database would need to be stored at each location participating in the network, and the data-storage and bandwidth requirements needed to operate such a system would be prohibitively large (Linn and Koo 2016). Instead, a blockchain technology-based medical system would likely need to function as a control for

accessing the data, noting where and when changes to medical records occur, rather than containing the entire dataset (Linn and Koo 2016). Blockchain databases can be designed so that large files, like x-rays, are “off the chain,” but the links to the files are stored “on chain” (Behlendorf 2017). Blockchain technology may be useful to generate an audit trail for particularly sensitive healthcare transactions, such as the prescribing of opioids. Given that medical information is worth 10 to 20 times more than credit card data on the dark web (Humer and Finkle 2014), privacy issues are also a concern for blockchain technology in healthcare (Cuomo 2016). Jerry Cuomo, IBM’s Vice President of Blockchain Technologies, said “within healthcare, more extensive privacy protections are needed . . . One goal is to ensure that institutions and individuals can only access information they’re supposed to see. A key element is ‘entitled access,’ which is achieved by using modern cryptography so access to private data requires presentation of encryption keys/certificates held by authorised participants” (Cuomo 2016). Various solutions to the privacy issues posed by blockchain technology are available, however. For example, a patient’s medical data must be encrypted, and permission to read or write that data could be based on an encryption key only known to the patient or his or her healthcare provider (Linn and Koo 2016). Another possible solution is a fully private blockchain database, where permission to read or write to the database is controlled by one organisation (eg a regulatory body) (Buterin 2017).

You might also like: Finance Technology Blockchain in Healthcare IT Security

While there are workable solutions to the technological challenges of blockchain implementation in healthcare, finding solutions to the regulatory challenges will require a greater collaborative effort by the healthcare industry and will likely require action by healthcare regulators. For example, traditional blockchain implementation may not be HIPAA compliant without additional measures (LaFever 2016). Blockchain technology relies on mathematically derived pseudonyms to verify the data on a distributed ledger (LaFever 2016). HIPAA privacy rules may forbid this practice because the pseudonyms pose a risk of potential re-identification of de-identified protected health information (PHI) (LaFever 2016). If PHI is contained in and passed in a blockchain database, would hundreds of business associate agreements be required to exchange healthcare data under HIPAA?

Blockchain implementation also raises other regulatory issues, including lack of an existing legal framework for regulating blockchain technology (Tena 2017), lack of an established legal authority or data governance that makes the rules and imposes sanctions, and finding ways to incentivise the sharing of patient data and reform efforts. Despite these regulatory challenges, there is evidence that regulators are taking notice, and change may be on the horizon.

For example, federal agencies, such as the Departments of Homeland Security, Justice and Treasury have been using blockchain services and contractors since 2015 and are now devoting increased resources towards blockchain innovation. Further, in 2016, the National Institutes of Health held a competition seeking white paper submissions on blockchain technology and its possible uses in healthcare (Linn and Koo 2016), and the FDA has partnered with IBM in the hope of developing “a secure, efficient, and scalable exchange of health data using blockchain technology” (IBM 2017).

The healthcare industry already has several blockchain initiatives under way, including a permissions management project for data from clinical trial patients, a patient-centric electronic health record on a permissionless blockchain database, a health identity blockchain database established by the Estonian government, and a blockchain-based healthcare claims management system (Behlendorf 2017).

Understanding risks

Adoption of blockchain technology in healthcare will require small test projects in exchanging and tracking data (Behlendorf 2017). Given the success of blockchain implementation in other regulated industries, such as the financial services industry, it makes sense to explore the opportunities for blockchain technology in healthcare, while also understanding the potential risks.

Sharon Klein and **Joe Guagliardo** are vice chairs of Pepper Hamilton’s Technology Group, a multipractice team that advises companies where technology is the business as well as companies where technology is critical to supporting the core business. Ms. Klein is also a member of the firm’s Health Sciences Department, a team of 110 attorneys who collaborate across disciplines to solve complex legal c hallenges confronting clients t hroughout the health sciences spectrum. Research assistance for this article was provided by summer associate John Melde.

Published on : Tue, 19 Sep 2017