Harvard Business Review

TECHNOLOGY

The Potential for Blockchain to Transform Electronic Health Records

by John D. Halamka, MD, Andrew Lippman, and Ariel Ekblaw

MARCH 03, 2017

A vexing problem facing health care systems throughout the world is how to share more medical data with more stakeholders for more purposes, all while ensuring data integrity and protecting patient privacy.

Traditionally, the interoperability of medical data among institutions has followed three models: push, pull, and view (discussed below), each of which has its strengths and weaknesses. Blockchain offers a fourth model, which has the potential to enable secure lifetime medical record sharing across providers.

Push is the idea that a payload of medical information is sent from one provider to another. In the U.S. a secure email standard called Direct is used to provide encrypted transmission between sender (for example, an E.R. physician) and receiver (for example, your primary care doctor). Although this has worked for health care providers in the past, it assumes that infrastructure is in place to actually make it work, such as the existence of an electronic provider directory for the community and a set of legal agreements enabling widespread sharing of data. Push is a transmission between two parties, and no other party has access to the transaction. If you end up being transferred to another hospital, the new hospital may not be able to access data about your care that was pushed to the first hospital. There is no guarantee of data integrity from the point of data generation to the point of data use — it is assumed that the sending system generated an accurate payload and the receiving system ingested the payload accurately — with no standardized audit trail.

Pull is the idea that one provider can query information from another provider. For example, your cardiologist could query information from your primary care doctor. As with push, all consent and permissioning is informal, ad hoc, and done without a standardized audit trail.

View is the idea that one provider can view the data inside another provider's record. For example, a surgeon in the hospital operating room could view an X-ray you had taken at an urgent care center. Security approaches are ad hoc, not audited in a standardized way, and not necessarily based on an existing patient-provider relationship.

All of these approaches work technologically, but the policies surrounding them are subject to institutional variation, local practice, state laws, and the rigor of national privacy policy enforcement.

Blockchain is a different construct, providing a universal set of tools for cryptographic assurance of data integrity, standardized auditing, and formalized "contracts" for data access.

Here's the idea:

Blockchain was originally conceived of as a ledger for financial transactions. Every financial institution creates a cryptographically secured list of all deposits and withdrawals. Blockchain uses public key cryptographic techniques to create an append-only, immutable, time-stamped chain of content. Copies of the blockchain are distributed on each participating node in the network.

How Blockchain Works

Here are five basic principles underlying the technology.

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

Today humans manually attempt to reconcile medical data among clinics, hospitals, labs, pharmacies, and insurance companies. It does not work well because there is no single list of all the places data can be found or the order in which it was entered. We may know every medication ever prescribed, but it can be unclear which medications the patient is actually taking now. Further, although data standards are better than ever, each electronic health record (EHR) stores data using different workflows, so it is not obvious who recorded what, and when.

Imagine that every EHR sent updates about medications, problems, and allergy lists to an open-source, community-wide trusted ledger, so additions and subtractions to the medical record were well understood and auditable across organizations. Instead of just displaying data from a single database, the EHR could display data from every database referenced in the ledger. The end result would be perfectly reconciled community-wide information about you, with guaranteed integrity from the point of data generation to the point of use, without manual human intervention.

they're linked to every transaction record that came before them (hence the term "chain"). Various 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.

My colleagues at the MIT Media Lab and Beth Israel Deaconess Medical Center tested this concept with medications, proving the viability of such an approach. In our white paper, "A Case Study for Blockchain in Healthcare," we proposed a novel, decentralized record management system to handle EHRs using blockchain technology, which we called MedRec.

MedRec doesn't store health records or require a change in practice. It stores a signature of the record on a blockchain and notifies the patient, who is ultimately in control of where that record can travel. The signature assures that an unaltered copy of the record is obtained. It also shifts the locus of control from the institution to the patient, and in return both burdens and enables the patient to take charge of management. For those patients who do not want to manage their data, I imagine that service organizations will evolve to serve as patient delegates for this task. One challenge of the project and the idea is building an interface that can make this responsibility palatable for patients. Most of the individual patient portals that people use today have cumbersome designs, create more work, and have different user interfaces at every institution. A deployed MedRec system would feature a user interface to simplify patient interaction with health care records that bridge multiple institutions.

As our next step, we plan to enhance the MedRec pilot with more data types, more data contributors, and more data users. We'll also consider innovative alternatives to existing blockchain implementations, such as Silvio Micali's Algorand public ledger, which requires much less computing power than other approaches.

The rationale for considering a blockchain in electronic health care records is twofold. First, it avoids adding another organization between the patient and the records. It is not a new clearing house or "safe deposit box" for data. The blockchain implies a decentralized control mechanism in which all have an interest, but no one exclusively owns it. This is an architectural change that generalizes past

medical records. Second, it adds due consideration to a time-stamped, programmable ledger. That opens the door for intelligent control of record access without having to create custom functionality for each EHR vendor. The ledger also inherently includes an audit trail.

One outcome we can all hope for is that blockchain continues to be developed at a disinterested, nonprofit university so that the idea can mature before it's optimized for commercial purposes. Blockchain for health care is very early in its lifecycle, but it has the potential to standardize secure data exchange in a less burdensome way than previous approaches.

John D. Halamka, MD, is CIO at Beth Israel Deaconess Medical Center.

Andrew Lippman is a senior research scientist at the MIT Media Lab.

Ariel Ekblaw is a graduate student at the MIT Media Lab.

This article is about TECHNOLOGY

⊕ **FOLLOW** THIS TOPIC

Related Topics: HEALTHCARE

Comments

Leave a Comment

8 COMMENTS

Berl Kaufman 14 days ago

The latest buzzword is "blockchain," and I agree that this technology is a great technical solution, but most of what the author says is really not about the technical implementation, but rather about the concept of a central repository for medical records. As a patient I am truly amazed that whenever I visit a physician for the first time they ask me for my medical history. That history is always imprecise. If my own history is imprecise, one can imagine how bad my family history is! You have to wonder whether physician take anything a patient says seriously given the manual nature of this task.

Speaking of family history, a terrific addition to this database would be a way of linking family records together. So when a physician checks my database she also sees all the relationships. Think about the potential for epidemiological research, where a researcher, given access anonymized data, could examine whole communities, towns, regions effortlessly. Tack on DNA test results to the database and you have almost a miraculous tool for the researcher.

Potentially there would be massive amounts of data for each patient, impossible for any given physician to properly analyze. That's where analytical computing engines come in. Especially useful for analyzing medication interactions. The engine would consist of a set of APIs that would examine the blockchain looking for contraindications, making recommendations, even potentially making diagnoses. No physician, no matter how well trained or experienced, could perform this sort of analysis effectively given the volume of data.

REPLY 0 0

JOIN THE CONVERSATION