Reinhart

The Benefits of Blockchain: How the Technology is Transforming Healthcare Cybersecurity

In 2017, there were at least 477 healthcare data breaches reported to the U.S. Department of Health and Human Services ("HHS") or the media, affecting 5.579 million patient healthcare records.[1] These breaches cost approximately $408 per record—more than 2.75 times the global average across industries.[2] Partially in response to this ongoing issue, healthcare technology innovators are exploring the use of blockchain to establish a more secure, integrated healthcare recordkeeping system.

Blockchain is a promising cybersecurity tool because of its decentralization and inherent security features. Many large companies and research institutions, IBM, MIT and Walmart, for example, are already working to implement blockchain into healthcare recordkeeping.

What is a Blockchain?

The most commonly known blockchains underlie cryptocurrencies—such as Bitcoin and Ethereum. The blockchain technology itself has broad applications.

A blockchain is a chain of blocks secured by cryptographic techniques. More specifically, it is a chain of blocks comprised of information recorded on a continuous, distributed (decentralized) digital ledger to which a new block can only be added once it is verified by the consensus of the parties to the ledger. Consensus methods vary by blockchain. For example, Bitcoin relies on miners to validate blocks by performing a proof-of-work algorithm as a vote towards consensus. Each block in the chain contains a unique hash, for example, a number in a consecutive list of numbers, as well as the hash of the preceding block.

A Promising Healthcare Cybersecurity Tool

Blockchain offers many cybersecurity benefits that address some of the endemic needs of the healthcare industry. These include consensus by consortium, individual record security, universal auditing and smart contracts.

One method of consensus that may work particularly well for healthcare entities is consortium. In this model, only a group of pre-defined trusted parties have access. This model could allow restricted access and limited permissions among

POSTED:

Oct 2, 2018

RELATED PRACTICES:

Health Care
https://www.reinhartlaw.com/practices/health-care

RELATED SERVICES:

Health Care Technology and Innovation
https://www.reinhartlaw.com/services/health-care-technology-and-innovation

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

groups of healthcare entities.

The digital architecture of blockchain as a decentralized chain of blocks is an innate security benefit. Records are currently often held in one digital repository such that if the repository is compromised, thousands of patient records may be breached. With a blockchain of patient records, hacking of the encryption key to one patient's record can limit harm because the hacker would need to obtain the unique encryption key of each member to access identifiable information. Even if this were accomplished, the hacker would have to repeat the process for *every* patient. This helps prevent massive, multi-patient breaches.

An additional critical feature of blockchain technology is that every member of a blockchain generally can access and audit the entire ledger. This allows all interested parties to confirm and update the information contained in individual blocks.

Another significant benefit is that laws and regulations can be programmed into the blockchain as smart contracts. Smart contracts are logical rules programmed into the blockchain. They are self-executing contracts where the built-in agreement is enforced on all members. Smart contracts mimic traditional contracts and laws, and can be used to program in obligations and consequences. In this way, the requirements of specific data privacy and security laws, such as the Health Insurance Portability and Accountability Act of 1996 or the European Union General Data Protection Regulation, can be embedded in the blockchain.

Innovators are already experimenting with blockchain use cases in the healthcare context that demonstrates many of the blockchain security benefits. Researchers at the MIT Media Lab have developed a prototype system called MedRec, an open-source prototype that applies blockchain smart contracts to create a decentralized content-management system for healthcare data.[3] The MedRec pilot program illustrated that the system disperses authorization data across participating entities, rather than creating a central target for attacks. MedRec is one example among many use cases demonstrating blockchain's ability to strengthen data security vulnerabilities in the healthcare industry.

If you or your company have data security compliance questions, please contact a member of Reinhart's Data Privacy and Cybersecurity group.

[1] Proteus 2017 Breach Barometer Annual Report. (2018). Retrieved September 30, 2018, from

https://www.protenus.com/press/press-release/56m-patient-records-breached-in-2017-as-healthcare-struggles-to-proactively-protect-health-data.

[2] IBM 2018 Cost of Data Breach Study. (2018). Retrieved September 30, 2018, from https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf.

[3] MIT Media Lab "MedRec: A Case Study for Blockchain in Healthcare." Available at: https://dci.mit.edu/research/blockchain-medical-records. Accessed September 30, 2018.