Blockchain Technology
Applications in Health Care

Suveen Angraal, MBBS; Harlan M. Krumholz, MD, SM; Wade L. Schulz, MD, PhD

Blockchain technology has gained substantial attention in recent years with increased interest in several diverse fields, including the healthcare industry. Blockchain offers a secure, distributed database that can operate without a central authority or administrator. Blockchain uses a distributed, peer-to-peer network to make a continuous, growing list of ordered records called blocks to form a digital ledger. Each transaction, represented in a cryptographically signed block, is then automatically validated by the network itself. Blockchain has also garnered interest as a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing. In this article, we describe the basics of blockchain and illustrate current and future applications of this technology within the healthcare industry.

Technical Background

Bitcoin, a cryptocurrency and payment system first introduced in 2008, is one of the most well-known implementations of blockchain.[1] The transfer of digital assets, such as bitcoin, within a blockchain is initiated when a seller or payer submits a transaction (Figure [A]).[2] These transactions are broadcasted to every peer connected to the blockchain network where clients, called miners, use a cryptographic algorithm to validate the transaction. This validation solves 2 key problems that previously existed with digital currency exchange: ensuring that the digital asset exists and that it has not already been spent. A transaction is said to be valid if a miner deems it is well formed (the input and output contain only the fields that are defined in the protocol), and the outputs it attempts to transfer exist. Miners are not certified and can be anyone who volunteers to invest their resources. The incentive for miners comes in the form of the bitcoin, which are generated and rewarded to the miners for every block of transactions validated. The software required to mine is free to download and simple to run. Once a transaction is validated by a configurable number of clients, it is stored in a block, which contains the details of validated transactions, along with a time stamp and a cryptographic hash (a mathematically generated alphanumeric string) of the data. The block with the transaction information is added to the end of the blockchain, which is followed by the transfer of assets to the receiving party. The one-way, cryptographic hash is an important aspect of the blockchain because this value forms a distinct, digital signature that is unique to the current block of data and is created using the hash of the block preceding it (Figure [B]). Because every block is securely linked to the block preceding it using the hash, malicious changes are prevented from being made to the blockchain ledger. The immutability is a key property of blockchain.

This approach has several practical differences compared with traditional transaction processing. For example, when a credit card transaction is initiated, a merchant's payment processor verifies available funds, and after several days, funds are approved and transferred to the merchant. The goal of blockchain as a digital ledger is to remove these intermediaries by establishing a digital trust that leads to more efficient transaction processing. In a blockchain environment, the network itself validates the transaction, secures the transaction history, and allows for assets to be transferred directly between parties once digitally validated.

Blockchain Applications

The use of blockchain for decentralized data management holds potential for applications beyond financial services. An article published in the Harvard Business Review highlights several potential applications of blockchain, from the validation of artwork to verification of voting records.[3] Because of this diverse interest, several companies, including IBM, Microsoft, Accenture, and others, have formed organizations to develop blockchain-based technology that can be adopted by industry partners.[4] Several companies have started to build on this technology for use cases that include identity verification, trade settlements, and supply chain management. This interest is largely driven by the prediction that the automation offered by blockchain-enabled software could save the financial service industry $15 to $20 billion annually within the next 5 years.[5]

Healthcare Applications of Blockchain

This interest and momentum has now extended to healthcare information technology. Realizing the potential relevance and importance of blockchain in health care, the Office of the National Coordinator for Health Information Technology,

From the Center for Outcomes Research and Evaluation, Yale New Haven Hospital, CT (S.A., H.M.K., W.L.S.); Section of Cardiovascular Medicine, Department of Internal Medicine (H.M.K.) and Department of Laboratory Medicine (W.L.S.), Yale School of Medicine, New Haven, CT; and Department of Health Policy and Management, Yale School of Public Health, New Haven, CT (H.M.K.).

Correspondence to Wade L. Schulz, MD, PhD, Center for Outcomes Research and Evaluation, Yale New Haven Health, 55 Church St, Suite 401, New Haven, CT 06510. E-mail wade.schulz@yale.edu

(*Circ Cardiovasc Qual Outcomes.* 2017;10:e003800. DOI: 10.1161/CIRCOUTCOMES.117.003800.)

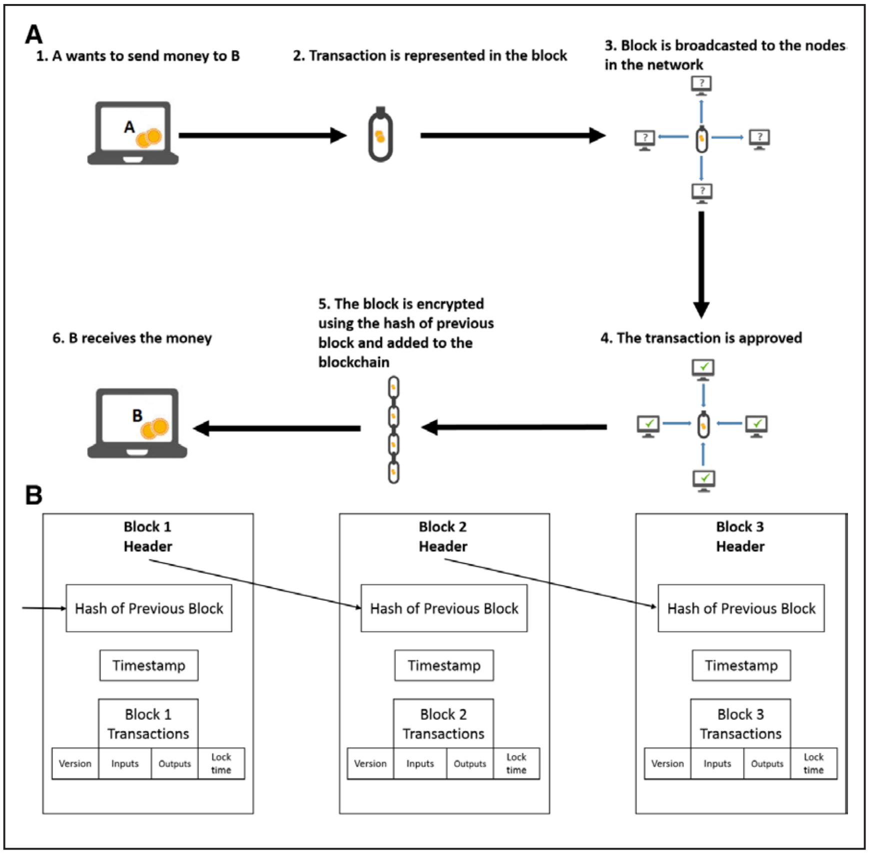

Figure. The execution of a transaction in blockchain (**A**) and the representation of a block in the blockchain (**B**).

in 2016, organized an ideation challenge for soliciting white papers on the potential use of blockchain in health care. This challenge resulted in several proposed healthcare applications for blockchain. While storing the entire health record within the blockchain could be envisioned as a use case for health care, several potential barriers to implementation have been identified, including concerns with privacy, compliance with regulatory requirements, and the technical barriers related to data storage and distribution. Because of this, most short-term proposals have focused on data validation, auditing, and authorization.

One implementation example is Guardtime, a Netherland-based data security firm, which partnered with the government of Estonia to create a blockchain-based framework to validate patient identities.[6] All citizens were issued a smartcard, which links their EHR data with their blockchain-based identity. Any update in the EHR is assigned a hash and registered in the blockchain. This approach ensures that data within the EHR contains an immutable audit trail and that records cannot be maliciously modified. The immutable, time-stamped data logs can also archive the state of information from existing healthcare databases. Any update in the healthcare database, like appointment scheduling, is assigned a time stamp and cryptographically signed in a block. Given the recent attention to data integrity because of concerns about scheduling fraud at the Veterans' Administration and the risk for data manipulation of implantable medical devices, such as pacemakers, such a system has several potential benefits to guarantee that any modifications to the healthcare record are secure and auditable.

A second EHR-related implementation is MedRec, a project started between MIT Media Lab and Beth Israel Deaconess Medical Center. This platform offers a decentralized approach to managing permissions, authorization, and data sharing between healthcare systems.[7] The use of blockchain in this application is intended to give patients the ability to have agency over and knowledge of who can access their healthcare data. These permissions can be shared on a blockchain to create a more automated approach to data sharing for clinical and research use, even though the actual healthcare data are not stored in the blockchain. While the permissions, data storage location, and audit logs are maintained in the blockchain, all healthcare information remains in EHR systems and requires additional software components to enable true interoperability.[7] The MedRec project has been tested as a proof of concept with medication data, and the developers are looking to enhance the project's scope by adding more data types, data contributors, and users. As shown by this proof of concept, biomedical and outcomes research may significantly benefit from the application of blockchain to provide rapid, secure access to longitudinal research data.

Unlike the use cases described to date, which have developed production software or proof-of-concept applications, most examples of blockchain remain in the concept stage. One such concept is supply chain management, where blockchain could be used to streamline management and increase efficiency by creating a formal registry to track products and components through every step of the process. Within health care, software based on blockchain could be developed to ensure the transparency of components used to manufacture medications, track medication distribution, and ensure the authenticity of prescriptions. Some of these use cases have already seen commercial interest, particularly for compliance with the Drug Supply Chain Security Act, which makes it necessary to provide lot-level product tracing and manufacturing history.[8]

Similar to processing trade settlements, blockchain has the potential to be used for the automated validation of claims, which may increase the efficiency and security of the process.[9] The software can store encrypted patient identifiers, health plan information, and provider claims within a blockchain that is shared by payers and providers. With this setup, near real-time automatic claims processing, eligibility verification, and preauthorization could become a reality. With appropriate permissions, researchers could also be given access to subsets of these data for use in biomedical research.

Technical Limitations of Blockchain

Several potential disadvantages exist compared with traditional data storage approaches, including potential issues with the distribution of personally identifiable healthcare data within a public ledger, scaling the blockchain, and the cost-effectiveness of implementation. First, while data within the blockchain can be deidentified and encrypted, distributed access to the entire data set does have the risk for potential compromise or reidentification. Second, the speed and scalability of a completely distributed system would also need to be addressed because concerns have already arisen in smaller blockchain-based applications.[10] Within a blockchain deployment, it is assumed that all blocks are stored on every client node within the system. As an illustration of this potential bottleneck, fully participating as a miner in the bitcoin network requires user to download the entire bitcoin ledger, which totaled ≈101 gigabytes at the end of 2016. In addition, the maximum rate of transaction validation within the bitcoin network is ≈7 transactions per second, which could limit the throughput of large blockchain networks.[10] The cost-effectiveness of such a platform that holds significantly larger volumes of data has yet to be proven in production environments. The combined expenditures for hardware, implementation, and support will need to be assessed to determine whether a return on investment for this technology can be realized. Such barriers make an argument that while blockchain has the ability to provide transparency and authenticity to data transactions, rapidly transitioning current healthcare IT systems to blockchain-based technology may be difficult.

Conclusions

Blockchain technology offers a platform that could be used for many potential applications in health care. While in the early stages of design and development, many organizations have proposed solutions that have the potential to increase healthcare data transparency and operating efficiency. However, the scalability, security, and cost-effectiveness of blockchain technology will require further research prior to large-scale production deployments. The future of this technology in healthcare and other industries is still being written, and the applications in research and clinical care are not yet established. Nevertheless, a distributed system that eliminates intermediaries has substantial potential to disrupt many current processes in health care and research.

Disclosures

Dr Schulz is the technical consultant to Hugo, a personal health information platform. Dr Krumholz is a recipient of research agreements from Medtronic and from Johnson & Johnson (Janssen), through Yale, to develop methods of clinical trial data sharing; is a recipient of a grant from Medtronic and the Food and Drug Administration, through Yale, to develop methods for postmarket surveillance of medical devices; works under contract with the Centers for Medicare & Medicaid Services to develop and maintain performance measures that are publicly reported; chairs a cardiac scientific advisory board for UnitedHealth; is a participant/participant representative of the IBM Watson Health Life Sciences Board; is a member of the Advisory Board for Element Science and the Physician Advisory Board for Aetna; and is the founder of Hugo. The other author reports no conflicts.

References

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf. Accessed January 15, 2017.
2. Forrest P. Blockchain and non financial services use cases. *Linkedin*. 2016. https://www.linkedin.com/pulse/blockchain-non-financial-services-use-cases-paul-forrest. Accessed May 28, 2017.
3. Tapscott D, Tapscott A. The impact of the blockchain goes beyond financial services. *Harvard Business Review*. 2016. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services. Accessed January 25, 2017.
4. Popper N. Business giants to announce creation of a computing system based on Ethereum. *The New York Times*. 2017. https://www.nytimes.com/2017/02/27/business/dealbook/ethereum-alliance-business-banking-security.html. Accessed March 1, 2017.
5. Belinky M, Rennick E, Veitch A. The Fintech 2.0 Paper: rebooting financial services. *Santander InnoVentures*. 2015. http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf. Accessed March 1, 2017.
6. Mettler M. Blockchain technology in healthcare: the revolution starts here. IEEE 18th International Conference on e-Health Networking, September 14–16, 2016. Piscataway, NJ: IEEE. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749510. Accessed March 3, 2017.
7. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD), August 22–24, 2016. Piscataway, NJ: IEEE. http://ieeexplore.ieee.org/abstract/document/7573685/. Accessed March 3, 2017.
8. Baunm S. Health IT startups working to secure pharma supply chains? *Medcity News*. http://medcitynews.com/2017/01/drug-supply-chain-security-and-technology/. Accessed March 1, 2017.
9. Witchey NJ. Healthcare transaction validation via blockchain proof-of-work, systems and methods. US patent US20150332283 A1. 2015.
10. Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Sirer EG, Song D. On scaling decentralized blockchains. International Conference on Financial Cryptography and Data Security. Berlin: Springer; February 26, 2016. https://link.springer.com/chapter/10.1007/978-3-662-53357-4_8. Accessed March 3, 2017.

Key Words: attention ■ database ■ health care ■ maintenance ■ patient-centered care