Medical Reference Services Quarterly

ISSN: 0276-3869 (Print) 1540-9597 (Online) Journal homepage: http://www.tandfonline.com/loi/wmrs20

An Introduction to the Blockchain and Its Implications for Libraries and Medicine

Matthew B. Hoy

To cite this article: Matthew B. Hoy (2017) An Introduction to the Blockchain and Its Implications for Libraries and Medicine, Medical Reference Services Quarterly, 36:3, 273-279, DOI: 10.1080/02763869.2017.1332261

To link to this article: https://doi.org/10.1080/02763869.2017.1332261

MEDICAL REFERENCE SERVICES QUARTERLY
2017, VOL. 36, NO. 3, 273–279
https://doi.org/10.1080/02763869.2017.1332261

Routledge
Taylor & Francis Group

EMERGING TECHNOLOGIES
Matthew B. Hoy and Tara J. Brigham, Column Editors

An Introduction to the Blockchain and Its Implications for Libraries and Medicine

Matthew B. Hoy

Libraries, Mayo Clinic, Rochester, Minnesota, USA

ABSTRACT
The blockchain is a relatively new technology used to verify and store transaction records for online cryptocurrencies like Bitcoin. The system is redundant and distributed, making it difficult for transactions to be rescinded, duplicated, or faked. Beyond online currencies, the blockchain has potential uses in health care, education, and many other fields. This column will briefly describe what the blockchain is and how it is being used, potential future uses that may be of interest to librarians and medical practitioners, and some of the problems with the system.

KEYWORDS
Bitcoin; blockchain; cryptocurrency; libraries; medical records

Introduction

As life increasingly moves online, one of the challenges Internet users face is conducting financial transactions in a setting where they cannot know or trust the other party. Some of these trust issues have been alleviated through the development of "cryptocurrencies" like Bitcoin. Bitcoin is a decentralized currency, first described in 2008, that exists entirely as "unique strings of letters and numbers" stored online.[1] All transactions in the Bitcoin economy are tracked in a ledger system called the "blockchain"; multiple copies of this ledger exist and are constantly compared to each other to ensure that all transactions are legitimate and properly recorded. There are many other cryptocurrencies similar to Bitcoin, but all use a similar type of blockchain ledger verification system.

While cryptocurrencies are an interesting and important topic, the blockchain ledger itself has many other potential uses outside of currency markets, including creating tamper-proof documents, distributed ownership records, and universal medical records. This article will briefly describe the blockchain, how it is currently being used, potential future uses that may be of interest to librarians and medical professionals, and some of the problems and barriers to implementation facing blockchain systems.

CONTACT Matthew B. Hoy hoy.matt@mayo.edu Mayo Clinic, 200 1st St SW, Rochester, MN 55905, USA.
Comments and suggestions should be sent to the Column Editors: Matthew B. Hoy (hoy.matt@mayo.edu) and Tara J. Brigham (Brigham.Tara@mayo.edu).

What is the Blockchain?

The blockchain is a key part of the infrastructure underlying Bitcoin and other cryptocurrencies. Wang and Vergne describe cryptocurrencies as "digital tokens that can be exchanged online, using cryptographic hashing and digital signatures to verify transactions and avoid double-spending of the same token."[2] Put more simply, cryptocurrencies are online, digital payment systems based on peer-to-peer networking technology and public key cryptography. These systems allow users to exchange value in a trustless setting: transactions are semi-anonymous, irrevocable, and each transaction is recorded in a distributed ledger that ensures all parties can agree that the transaction happened. Marc Andreessen, a well-known venture capitalist, calls cryptocurrencies

> a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer.[3]

The theory behind Bitcoin was first explained in a 2008 white paper written under the pseudonym "Satoshi Nakamoto."[4] Almost a decade later, "Nakamoto" has still not been definitively identified, although there is compelling evidence he is an Australian cryptanalyst.[5] Despite the unknown identity of its creator, Bitcoin has seen rapid development and adoption as an online payment system, particularly for transactions that require anonymity, are vulnerable to fraud, or are legally questionable. Bitcoin is currently the most popular cryptocurrency, but there are many others; popular examples include Litecoin, Peercoin, Ripple, and Ethereum.[2]

Cryptocurrencies have no central issuing authority and are not backed by any government or commodity. They are predicated on the idea that value comes from scarcity and the amount of effort required to obtain a scarce item. The blockchain is a key to making this scarcity possible. Not only does the blockchain keep a redundant, distributed record of all transactions, but it also helps generates the value in the cryptocurrency system. In the Bitcoin system, people referred to as "miners" provide the computing power to compile, store, and verify the blockchain ledgers; in exchange, they receive small amounts of Bitcoin for each transaction they verify. These verifications involve solving complex computations called "proof-of-work."[4] By forcing the miners to invest energy and expensive computer hardware in generating the proof-of-work, the blockchain embeds the value of that work in the Bitcoins the miners are paid. The value of Bitcoins is also bolstered by their limited availability: the system is designed in such a way that there will never be more than 21 million Bitcoins, and they are being slowly added in a controlled manner to prevent deflation. Bitcoin is already a major component of the online economy; current estimates of the total value of all Bitcoins in existence

hovers around $20 billion.[6] Many online retailers accept Bitcoin, and there are many mechanisms for exchanging fiat currency for Bitcoins and vice versa.[7]

While Bitcoin and other cryptocurrencies are important and interesting, they are not the main focus of this column. The idea of the blockchain ledger, the distributed and tamper-proof record of all the transactions made in the Bitcoin economy, has implications that reach far beyond just moving around imaginary pieces of currency.

Why is the Blockchain Important?

Bitcoin has already shown there is a place for a currency system that is decentralized and open. There are many other systems in society that could be updated and improved with a similar public ledger system. Some are hailing the blockchain as a fundamental new technology layer that could revolutionize the future of transaction-based exchanges, similar to the way new networking protocols in the early days of the Internet allowed for the growth of systems like the World Wide Web and today's media streaming services. The main distinction between those early network protocols and the blockchain, as Bheemaiah points out, is that "TCP/IP allowed information to be transmitted instantly … the blockchain protocol allows the instant transfer of value."[8]

In her book *Blockchain, Blueprint for a New Economy*, Melanie Swan forecasts three phases of blockchain adoption: Blockchain 1.0, 2.0, and 3.0. She defines Blockchain 1.0 as the online cryptocurrency phase, exemplified by the current Bitcoin system. We are already well into this phase, as evidenced by the thousands of Bitcoin transactions taking place every day. Blockchain 2.0 is in the near future: it expands to encompass tracking contracts, financial records, public records, and ownership of property in the blockchain. Examples of Blockchain 2.0 systems include fraud- and error-resistant land ownership records databases.[9] Swan's vision for Blockchain 3.0 expands into science, medicine, and education. She predicts that the blockchain will move information that has been hidden and controlled within institutions to open and distributed blockchains.[10] These possible uses should be the most intriguing to readers of this column. The next two sections will explore the implications the blockchain may have for medicine and libraries.

How Will the Blockchain Affect Medicine?

Although medicine sometimes lags behind other industries in adopting new technologies, there may be reasons to embrace the blockchain in health care sooner rather than later. Managing electronic medical records in the blockchain could have several advantages. Swan notes that patient records stored

this way could "be analyzed but remain private, with an embedded economic layer to compensate data contribution and use." She also mentions the research potential of large blocks of health data in a structured format; she envisions "a standardized secure mechanism for digitizing health data into health data commons," where patients could make their structured data available to researchers in exchange for a cryptocurrency embedded in the record system.[10]

Others are also advocating for blockchain-based patient health care data systems; researchers claim these systems would improve privacy and security by placing control of the data in patients' hands, allowing them to grant and revoke access to their medical records as needed.[11,12] Placing control of the record in patients' hands may create other issues, but it could also improve care since each provider the patient visits would be able to access the same complete set of records, and patients are more likely to be engaged in their care when they manage their own records.

Another potential medical use for the blockchain was identified by Mackey and Nayyar; they proposed using the blockchain to combat drug counterfeiting. They see potential in using the system to track drugs through the entire manufacturing and distribution process, developing counterfeit detecting devices, and allowing participants to share data across manufacturers and supply chains.[13]

How Will the Blockchain Affect Libraries?

Basically, the blockchain is about storing information in a distributed, tamper-resistant setting. This fits well with the work librarians have always done, that is, gathering, preserving, and sharing authoritative information. The blockchain can help librarians achieve that work, especially in the world of scientific publication. One potential use for the blockchain is to create timestamped, verifiable versions of journal articles. Irving and Holden successfully tested the use of the Bitcoin blockchain "as a low cost, independently verifiable method that could be widely and readily used to audit and confirm the reliability of scientific studies."[14] They did this by creating a cryptographic hash of the plaintext of a trial protocol document and using that hash to create a new private Bitcoin key. This creates a time-stamped record in the blockchain, which other researchers can quickly verify in the future. If the document has been changed, the hash of the new document will not match the one stored in the blockchain.

Another potential use for the blockchain in libraries is as a digital rights management (DRM) tool. Digital resources are inherently reproducible, and this creates issues for libraries and publishers. Publishers have imposed draconian, often unworkable DRM tools on libraries and consumers in order to prevent copying of their materials. Because the blockchain creates a unique,

verifiable record that can be accessed by anyone, it could be tied to digital materials and used as a method to show "proveable scarcity" of that resource. This would allow digital materials to be uniquely identified, controlled, and transferred.[15] Publishers could be reassured no copies were being made, but whether prices would decrease accordingly is debatable.

The blockchain also has implications for education in general. Just as a blockchain medical record would place control of data in patient's hands, a blockchain education record could allow students to have a verifiable history of their academic achievements that they control. At least one company is actively pursuing such a system. Early in 2016, Sony announced plans to build a blockchain for the "open and secure sharing of academic proficiency and progress records."[16]

What's the Matter with the Blockchain?

The blockchain is not without its problems. The technical complexity of the cryptography and networking involved can make it difficult to understand. If we apply the blockchain to our current systems, this complexity may have negative consequences that far outweigh any benefits it delivers. Many patients have trouble navigating the health care system now; asking them to take on managing their own records in a complex blockchain setup is not likely to improve their care. Likewise, any use of the blockchain in the legal or education systems is going to require massive changes to industries that have a vested interest in keeping control of customers' data.

Another issue with current blockchain implementations is they are inefficient and environmentally unsustainable. The "proof-of-work" requirements in current versions of the blockchain require massive amounts of electricity; the energy cost of a single Bitcoin transaction could power 1.5 American homes for a day.[17] As the ledgers get longer, the math gets harder, and the amount of power being used increases. Thankfully, there are less computing-intensive versions of the blockchain in development.

Possibly the biggest problem with the blockchain is there is a great deal of hype, uncertainty, and fraud surrounding it. Cryptocurrencies in general, and Bitcoin in particular, have an image problem and are regarded as something used for nefarious or criminal purposes. When hackers use ransomware to seize computer networks, they demand payment in Bitcoin.[18] When people buy illicit drugs on the "dark web," they pay in Bitcoin.[19] When people see stories in the media mentioning cryptocurrencies being used to facilitate crime, it does not improve the image of the blockchain as a legitimate means of storing information or conducting business. Whether the blockchain can overcome this outlaw image and develop to its full potential as an information storage and verification system remains to be seen.

Conclusion

The blockchain ledger system was created as a component of cryptocurrency technology, but it has many other potential uses. In the near future, everything from medical records to library checkouts could be tied to a blockchain ledger containing verifiable time-stamped records of creation and ownership. These systems could also be used to transfer value between users, detect changes in documents, or prevent data tampering. Librarians and others working in the health care field should consider the systems and processes they currently use, and explore whether moving them to the blockchain could be beneficial.

Notes on Contributor

Matthew B. Hoy, MLIS, AHIP (hoy.matt@mayo.edu) is Associate Director of Libraries, Mayo Clinic, 200 1st St SW, Rochester, MN 55905.

References

1. Bohannon, John. "The Bitcoin Busts." *Science* 351, no. 6278 (March 2016): 1144–1146. doi:10.1126/science.351.6278.1144.
2. Wang, Sha, and Jean-Philippe Vergne. "Buzz Factor or Innovation Potential: What Explains Cryptocurrencies' Returns?" *PLOS ONE* 12, no. 1 (January 2017): e0169556. doi:10.1371/journal.pone.0169556.
3. Andreessen, Marc. "Why Bitcoin Matters." DealBook. January 21, 2014. https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.
4. Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed March 1, 2017. http://bitcoin.org/bitcoin.pdf.
5. Greenberg, Andy, and Gwern Branwen. "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius." *WIRED*. December 8, 2015. https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/.
6. Blockchain.info. "Market Capitalization." Accessed April 1, 2017. https://blockchain.info/market-cap.
7. Lischke, M., and B. Fabian. "Analyzing the Bitcoin Network: The First Four Years." *Future Internet* 8, no. 1 (March 1, 2016): Article number 7. doi:10.3390/fi8010007.
8. Bheemaiah, Kariappa. "Block Chain 2.0: The Renaissance of Money." *WIRED*. January 6, 2015. https://www.wired.com/insights/2015/01/block-chain-2-0/.
9. "The Great Chain of Being Sure about Things." *The Economist*. October 31, 2015. http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.
10. Swan, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, 2015.
11. Yue, X., H. Wang, D. Jin, M. Li, and W. Jiang. "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control." *Journal of Medical Systems* 40, no. 10 (August 26, 2016). 218. doi:10.1007/s10916-016-0574-6.
12. Xia, Qi, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments." *Information* 8, no. 2 (April 17, 2017). 44. doi:10.3390/info8020044.

13. Mackey, Tim K., and Gaurvika Nayyar. "A Review of Existing and Emerging Digital Technologies to Combat the Global Trade in Fake Medicines." *Expert Opinion on Drug Safety* 16, no. 5 (April 7, 2017). 587–602. doi:10.1080/14740338.2017.1313227.
14. Irving, Greg, and John Holden. "How Blockchain-Timestamped Protocols Could Improve the Trustworthiness of Medical Science." *F1000Research* 5, no. 222 (February 26, 2016). doi:10.12688/f1000research.8114.2.
15. Griffey, Jason. *Blockchain & Intellectual Property—Internet Librarian 2016*. October 18, 2016. https://speakerdeck.com/griffey/blockchain-and-intellectual-property-internet-librarian-2016.
16. "Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records." Sony Global, Sony Global Headquarters. February 22, 2016. http://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html.
17. Malmo, Christopher. "Bitcoin Is Unsustainable." Motherboard. June 29, 2015. https://motherboard.vice.com/en_us/article/bitcoin-is-unsustainable.
18. Pope, Justin. "Ransomware: Minimizing the Risks." *Innovations in Clinical Neuroscience* 13, no. 11–12 (November-December, 2016): 37–40. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/.
19. Broséus, Julian, Damien Rhumorbarbe, Caroline Mireault, Vincent Ouellette, Frank Crispino, and David Décary-Hétu. "Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organization from a Canadian Perspective." *Forensic Science International* 264 (July 2016): 7–14. doi:10.1016/j.forsciint.2016.02.045.