An Overview of Blockchain and Cryptocurrency in Healthcare and Orthopaedic Surgery

Evan M. Banks, BS[1] Alicia K. Harrison, MD[1,2] Allison J. Rao, MD[1,2]

[1]University of Minnesota Medical School, Minneapolis, MN [2]Department of Orthopaedic Surgery, University of Minnesota Medical School, Minneapolis, MN

Objectives: Analyze the current published literature and provide a high-level overview of blockchain technology in healthcare and orthopaedic surgery.

Design: Review.

Results: While the advantages of blockchain technology have been discussed extensively in the finance world, there are also many potential advantages for blockchain to be implemented in healthcare and orthopaedic practice. Some of these advantages include enhanced data security, research, remote patient monitoring, and supply chain tracking. However, many limitations with the current iterations of blockchain technology prevent its practical use.

Level of Evidence: Level IV; Review

Key Words: Blockchain, cryptocurrency, business, management, human resources, cost, value, efficiency

I. Introduction

What is blockchain, and how was this technology developed?

In 2008, Satoshi Nakamoto created a new peer-to-peer electronic cash transferring system that would allow online payments to be sent directly from one party to another without going through a financial institution.[1] This new technology would give rise to the first decentralized digital currency, (i.e. Bitcoin), allowing users to trade coins among participants in a distributed network without needing a centralized, trusted third party. This distributed ledger technology, also known as blockchain, has become more prominent in recent years as innovation has accelerated.

Application of Blockchain Technology in Healthcare

Although blockchain technology has been well-studied in the finance industry, its potential application extends far beyond trading cryptocurrencies. Recently, there has been increased interest in blockchain in the healthcare industry. Two previous systematic reviews identified numerous uses for blockchain in healthcare, including managing electronic medical records, biomedical research and education, remote patient monitoring, pharmaceutical supply chains, health insurance claims, health data analytics, and other potential areas.[2,3]

Purpose of the article

This article aims to provide a high-level overview of blockchain technology and its potential use in healthcare.

II. Defining Blockchain Technology

Basic Principles: Distributed Public Ledgers

Satoshi Nakamoto, an unknown person/entity/group, wrote a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" in October 2008. In it, Satoshi describes a "peer-to-peer electronic cash transferring system that would allow online payments to be sent directly from one party to another without going through a financial institution."[1] This underlying technological system allowing Bitcoin to function has come to be known as a blockchain. Bitcoin has become one of the most well-known uses of blockchain, and therefore, we cite it frequently during our explanation of blockchains, but we note that Bitcoin is only one implementation of blockchain. In its simplest form, a blockchain is a distributed public ledger or a record of all transactions that have ever taken place. Therefore, *Bitcoin's* blockchain is a distributed public ledger of *Bitcoin* transactions or a record of all transactions that have ever occurred. Ledgers are well-

known in the world of accounting and are nothing more than a collection of transactions and accounts.

Satoshi's critical innovation was making this ledger public and decentralized. Bitcoin's blockchain is public in that anyone can run the Bitcoin software to monitor and explore every Bitcoin transaction that has ever taken place.

Most importantly, Satoshi's innovation allowed these public ledgers to be decentralized. Anyone worldwide with a computer can download the Bitcoin software to help maintain the Bitcoin network and process transactions. This solution, which requires proper controls and alignment of incentives, is the true innovation of blockchains.

Blockchain: A Chain of Blocks

Blockchains are simply a chain of blocks of data. Each data block contains transactions, logs, files, etc., which are then encrypted and built on top of the prior block. The encryption mechanism ensures that each block is linked to the prior block, which is linked to the block before it, and so on. This encryption methodology ensures that editing data in one block would impact the entire blockchain. This "immutability" is a key feature of blockchains. This feature of blockchains harkens back to the core tenants of being public and decentralized: anyone around the world can verify the blockchain and ensure it has not been tampered with due to this chain of blocks and the fact that each is built on top of the prior.

No Need for Trusted Centralized Third Parties

The decentralization described above means that there is no need for a trusted centralized third party to maintain the blockchain. Instead of trusting a decentralized third party, you can trust the network itself. For example, when you want to know how much money is in your checking account, you ask your bank - a trusted centralized third party. The bank keeps a running ledger of all your transactions, and you trust the bank to be accurate and report your balance correctly. Blockchains enable you to shift that trust to the software itself. When you want to know how much Bitcoin you have, you can examine the public and open-source Bitcoin ledger.

It is important to note that removing trusted centralized third parties has pros and cons. For example, a benefit is that you are in complete control of your assets on a blockchain. A bank can seize your money, but with a blockchain, all you need to do is keep your private key a secret, and you are the only one who can access the funds.

Conversely, this complete control means there is no "undo button." Unlike a bank wire, if you accidentally send cryptocurrency to the wrong public address, you cannot get it back.

Usernames and Passwords

Rather than utilize usernames and passwords, cryptocurrency blockchains generally utilize public and private keys. A public key is akin to a username, and a private key is akin to a password. The public key is actually cryptographically derived from the underlying private key. For example, looking at the Bitcoin blockchain, the private key '5JU9Fyq1hwtg1YJnwshnxN1ffB7sFeKVJQnncKGoxwTBHTfTf9L' translates to public key '1L6ui1mKb6TzE3uojQe82yrwZhZXdJsC9H'. The Bitcoin blockchain uses a cryptographic algorithm known as SHA256,[6] which has 2^256 private keys. This means the odds of guessing someone's private key (i.e., password) are infinitesimally small.

The Blockchain Trilemma

Blockchains must wrestle with what is now famously known as the 'blockchain trilemma.' Blockchains must balance the trade-offs of optimizing for security, scalability, or decentralization. To date, no blockchain has been able to achieve all three.

Bitcoin, for example, prioritizes security and decentralization while sacrificing scalability. The

Bitcoin protocol can only process ~7 transactions per second,[7] and new blocks are added to the Bitcoin blockchain approximately every 10 minutes. This means that, on average, you will need to wait ~10 minutes to have your transaction confirmed on the Bitcoin blockchain, and even longer if you would like multiple confirmations.

Other blockchains try to improve on this scalability issue by sacrificing decentralization. For example, Visa and Mastercard both run blockchain-like databases that are secure and capable of processing tens of thousands of transactions per second.[8] However, these credit card databases are highly centralized and completely controlled by Visa and Mastercard. While blockchains are an exciting and new technology, they are not a solution to every problem. If your goal is speed and control, a centralized database is likely a better fit. However, if your goals are decentralization and transparency, then a blockchain is far superior to traditional databases.

Consensus Algorithms

A consensus algorithm is a set of rules or protocols that help a blockchain network agree on the current state of the network. Two dominant consensus algorithms have emerged to maintain the security of blockchains and process transactions: Proof of Work and Proof of Stake

Proof of Work

Proof of work is a consensus mechanism used in blockchain networks to validate and secure transactions and add new blocks to the blockchain. Proof of work, often referred to as "mining," was the consensus mechanism first utilized by Satoshi and the Bitcoin blockchain and subsequently replicated and modified by numerous other blockchains. In proof of work, computers, graphics cards, or specialized computer chips expend electricity to solve a cryptographic challenge akin to guessing lottery numbers. Whatever computer successfully guesses the correct number is granted the ability to create the next block in the chain and include whatever transactions it sees fit. Proof of work balances decentralization via the random selection of who gets to build the next block, combined with the alignment of incentives by imposing a cost (i.e., electricity) on participation in the network to dissuade any bad actors.

Proof of Stake

Proof of stake is a consensus mechanism whereby network participants 'stake' a portion of their coins as collateral, ensuring that they abide by the rules when building the next block of the blockchain. Stakers are randomly chosen by the blockchain software and given the opportunity to build the next block. However, if the block builder violates a rule of the blockchain, it can be challenged by other network participants, and the block builder's collateral can be confiscated as a penalty.[9]

Smart contracts

Beyond processing transactions and storing data, blockchains can also be used to execute software programs. These smart contracts are stored on the blockchain and executed automatically. For example, imagine a travel insurance contract that pays out if a hurricane occurs in a certain timeframe. The smart contract could define the critical sources of information, automatically check those sources, and automatically payout the insurance without any further human intervention required.

Types of Blockchain

While Bitcoin is one of the most well-known implementations of blockchain, several alternative blockchains are continually emerging with new innovations and ideas, as outlined below.[11]

Public blockchain:

These are open and permissionless blockchains accessible to anyone. Anyone can participate in the network, read the transactions, and validate blocks.

Examples include Bitcoin and Ethereum. Public blockchains are often used for cryptocurrencies and decentralized applications. In general, public blockchains prioritize decentralization and security over scalability.

Private blockchain:

Strict management of a network's data access authorization. These blockchains are typically used within organizations or consortia for purposes such as supply chain management, document verification, and internal record-keeping. Access control and data privacy are priorities in private blockchains. In other words, private blockchains sacrifice decentralization to gain scalability, privacy, and control.[12]

Permissioned blockchain:

Generally, private blockchains will evolve to be permissioned blockchains, which place rules on who is allowed to join the network and transact.

Consortium blockchain:

Consortium blockchains are a hybrid between public and private blockchains. They are operated and validated by a predefined group of organizations or entities, making them more scalable and efficient than public blockchains. Consortium blockchains are often used for industry-specific applications and collaborations among multiple stakeholders.

III. Blockchain uses in Health Care: A Vision for the Future

Blockchains enhance information storage and delivery by providing end-to-end and completely transparent data history. This allows data to be accessed by multiple parties, ensures full traceability and auditability, and opens the potential for new programmability and efficiency.[11] Blockchain provides opportunities to address various disciplinary systems issues, such as the Internet of Things (IoT),[18] supply chain management,[19] and Industry 4.0.[20] In this article, we focus on healthcare, which has numerous potential uses for blockchain.

Medical Records

Numerous articles have outlined the potential for blockchain technology to be used in the storage of medical records to decrease the risk of data compromise.[21,22] Articles have directly called out, "As a distributed ledger protocol composed of encrypted blocks of data organized in chains, blockchain represents a potential tool to solve the shortcomings of EHRs in terms of interoperability and privacy."[23] In theory, blockchains could allow for a completely interoperable EMR, with patients using their private key to selectively grant access to certain providers with time expirations. These "patient-centric" health records could provide a more complete view of a patient's health, and even potentially reduce the third leading cause of death in the US - medical errors.[24] Numerous third-party applications could be built on top of this master EMR blockchain, with some focused on patients and usability, while others focus on research and macro-insights. Insurance companies could also more closely track care and potentially process claims more efficiently. We recognize that a complete overhaul of the existing EMR ecosystem is highly unlikely, but blockchains open the door to improvements.

Credentialing

Diplomas, licenses, and certifications could be stored on a single credentialing blockchain, with new employees granting their new employer/hospital access to their records, greatly expediting the process.[25] Some articles estimate that "total estimated expenses and opportunity costs associated with licensure and certification occurring through completion of the first board recertification cycle for physicians is between $10,000 and $20,000."[26] This is likely driven by the multiple hours spent requesting paperwork and verifying

the paperwork. A single source of truth blockchain could reduce the need for data verification and utilize smart contracts to ensure the proper expiration of certifications and licenses. This problem is only larger in high-turnover or temporary positions such as locums or traveling nurses.

Remote Patient Monitoring

Blockchains could be used to monitor and record data from body and mobile devices outside of traditional healthcare environments, such as hospitals. Griggs et al. uses blockchain for smart contracts for automatic patient monitoring using Ethereum, the second biggest cryptocurrency by market capitalization after Bitcoin.[27] The cryptography and security of blockchains could ensure that only authorized parties are able to access the data, and the immutability of blockchains could ensure that the data is authentic.

Supply Chain Tracking

Liu et al. 2021 and Pane et al. 2020 describe the use of blockchain for drug and device tracking.[28,29] Supply chains have been investigating the benefits of blockchains for years, most notably when Walmart announced tracking lettuce suppliers using blockchain to quickly identify contamination.[30] The healthcare industry faces unique challenges to ensure the provenance, expiration, and authenticity of medical goods.[31] Blockchains could assist with arthroplasty or other implant registries to monitor for outliers in performance or revision rates.[29] Utilizing blockchain to track the creation and movement of goods can simultaneously improve safety while reducing the cost of tracking. A central blockchain repository tracking all medical goods could then be optimized across a system, state, and country. This blockchain could also allow for discovering new suppliers for organizations and could even enhance the speed and efficacy of recalls.

Automating Insurance

Blockchains could serve as a transparent and immutable neutral ground for insurers, pharmaceutical companies, medical device companies, and healthcare systems to come together and optimize payments. Contracts could be digitized and automated into smart contracts, which automatically execute and move money when certain triggers occur.[32]

Clinical trials

Omar et al. 2020 describe the use of blockchain in clinical trials.[33] They state, “The proposed framework results are advantageous to all stakeholders ensuring transparency, data integrity, and protocol compliance.” Blockchain could enable a world where patients could opt to reveal their anonymized data to researchers and be compensated directly for this data sharing. Blockchains could enhance the security of data, improve the accuracy of data, and allow for multiple analyses to be done on the same set of data (assuming patients grant access). Research could be greatly enhanced and accelerated thanks to global access to data, rather than having to cobble together local patient records.

IV. Blockchain uses in health Care: Limitations

The potential use cases of blockchain in healthcare continue to evolve every day. However, there are limitations in the current iterations of blockchain technology.

Scalability:

Healthcare data transactions continue to increase in size and volume, requiring increased computational bandwidth.[35] One disadvantage of current blockchain technology is the lack of transaction speed and scalability, which we previously discussed as the

"blockchain trilemma." Ethereum has a block size limit of around 12 megabytes (MB). In comparison, CT image sizes range from hundreds to thousands of megabytes. Storing such large image files on smaller block sizes would be technically inefficient. However, as blockchain technology continues to evolve, certain healthcare data, such as large images, could be kept off the blockchain. Each 'block' would keep a small amount of information to describe a specific patient or procedure and would serve to augment the existing EHR.[36]

Privacy and Security:

While blockchain technology can enhance the security of data without the need to worry about single-point failure, there are still ways in which attackers can gain access to a blockchain. Smart contracts that utilize traditional encryption systems may be susceptible to quantum attacks in which attackers undermine the security of a cryptographic system to extract a private or public key. To combat such attacks, quantum blind signatures, in which the signer cannot link the actual content of the message being signed, can enhance the security of a blockchain network.[37]

Interoperability:

While blockchain seeks to solve the interoperability challenge within a single healthcare system, one of the primary challenges of blockchain interoperability is the need for a standardized communication protocol across different blockchains, such as if multiple healthcare systems implement different blockchain technologies within their respective EMR.[38] To achieve interoperability, developers must create bridges or cross-chain communication protocols that can translate and securely transmit information between different blockchains. While Wang et al. 2023 identifies numerous potential solutions to this challenge, successful interoperability remains an ongoing area of research.[39]

V. Blockchain uses in health care: Ready for Orthopaedics?

While many of the potential benefits of blockchain technology previously discussed would apply to healthcare broadly, few studies have identified specific applications to the field of orthopaedic surgery. Thomson et al. 2021 systematically reviewed potential use cases within the current needs of orthopaedic practice.[34] They discuss potential uses within research and implant tracking.[34] However, they also acknowledge that current blockchain technology may not be able to implement the proposed uses practically and would require considerable capital investment in new infrastructure.[34] Though still in its early stages, blockchain technology has the potential to greatly enhance data security, research, and storage of medical data within an orthopaedic practice.

VI. Conclusion

Blockchains are decentralized public ledgers that remove the need for a trusted centralized third party. Their initial applications focused on finance and the movement of money, most notably Bitcoin and other cryptocurrencies. It is important to understand these technologies as they become increasingly mainstream, including the approval of a Bitcoin ETF. Cryptocurrencies are becoming more common in individual and institutional investor portfolios.

Blockchain uses extend beyond finance, with numerous use cases being pursued in healthcare. Blockchains allow for enhanced trust, improved security, and immutability of data. They could impact everything from medical records to credentialing to supply chains. It is critical to understand the fundamental benefits and limitations associated with blockchains so that we leverage their power in the near future.

Acknowledgements:

The authors would like to thank Adam M. Swick for his contributions to this manuscript.

REFERENCES

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*. Published online 2008. https://assets.pubpub.org/d8wct41f/31611263538139.pdf
2. Saeed H, Malik H, Bashir U, et al. Blockchain technology in healthcare: A systematic review. *PLoS One*. 2022;17(4):e0266462.
3. Elangovan D, Long CS, Bakrin FS, et al. The Use of Blockchain Technology in the Health Care Sector: Systematic Review. *JMIR Med Inform*. 2022;10(1):e17278.
4. Blockchain healthcare and life sciences solutions. Accessed January 26, 2024. https://www.ibm.com/blockchain/industries/healthcare
5. The Mempool Open Source Project®. Accessed January 16, 2024. https://mempool.space/
6. Brown K. Announcing approval of federal information processing standard (fips) 197, advanced encryption standard (aes). *J Res Natl Inst Stand Technol*. Published online 2002.
7. Chauhan A, Malviya OP, Verma M, Mor TS. Blockchain and Scalability. In: *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE; 2018:122-128.
8. Fujihara A. Check for updates Estimating the Relationship Between Block Size and Block Propagation Time in Bitcoin by Simulation. In: *Advances in Intelligent Networking and Collaborative Systems: The 15th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2023)*. Vol 182. Springer Nature; 2023:166.
9. Proof of stake vs proof of work: What you need to know. Published July 12, 2023. Accessed January 16, 2024. https://www.fidelity.com/learning-center/trading-investing/proof-of-work-vs-proof-of-stake
10. Proof-of-stake vs. proof-of-work: Pros, cons, and differences explained. Cointelegraph. Accessed January 26, 2024. https://cointelegraph.com/learn/proof-of-stake-vs-proof-of-work:-differences-explained
11. What is blockchain technology? Accessed January 26, 2024. https://www.ibm.com/topics/blockchain
12. Blockchain in the food supply chain - What does the future look like? Blockchain in the food supply chain - What does the future look like? Accessed January 16, 2024. https://tech.walmart.com/content/walmart-global-tech/en_us/news/articles/blockchain-in-the-food-supply-chain.html
13. Cryptocurrency prices, charts and market capitalizations. CoinMarketCap. Accessed January 26, 2024. https://coinmarketcap.com/
14. What is bitcoin mining? How does crypto mining work? Accessed January 26, 2024. https://www.fidelity.com/learning-center/trading-investing/crypto/what-is-mining
15. Top cryptocurrency exchanges Ranked by volume. CoinMarketCap. Accessed January 26, 2024. https://coinmarketcap.com/rankings/exchanges/
16. SEC.gov. Published January 10, 2024. Accessed January 26, 2024. https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023
17. Ward SV. Bitcoin Overtakes Silver As Second Largest ETF Commodity. *Forbes Magazine*. Published online January 24, 2024. Accessed January 26, 2024. https://www.forbes.com/sites/digital-assets/2024/01/24/bitcoin-overtakes-silver-as-second-largest-etf-commodity/
18. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener Comput Syst*. 2018;88:173-190.
19. Gao Z, Xu L, Chen L, Zhao X, Lu Y, Shi W. CoC: A unified distributed ledger based supply chain management system. *J Comput Sci Technol*. 2018;33(2):237-248.
20. Fernández-Caramés TM, Fraga-Lamas P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access*. 2019;7:45201-45218.
21. Shahnaz A, Qamar U, Khalid A. Using Blockchain for Electronic Health Records. *IEEE Access*. 2019;7:147782-147795.
22. Usman M, Qamar U. Secure Electronic Medical Records Storage and Sharing Using

Blockchain Technology. *Procedia Comput Sci*. 2020;174:321-327.
23. Han Y, Zhang Y, Vermund SH. Blockchain Technology for Electronic Health Records. *Int J Environ Res Public Health*. 2022;19(23). doi:10.3390/ijerph192315577
24. Study suggests medical errors now third leading cause of death in the U.s. - 05/03/2016. Accessed January 26, 2024. https://www.hopkinsmedicine.org/news/media/releases/study_suggests_medical_errors_now_third_leading_cause_of_death_in_the_us
25. Is blockchain the new pathway to credentialing? Accessed January 16, 2024. https://www.nursingcenter.com/ncblog/march-2020/blockchain-credentialing
26. Hansen DA, Mueller JT, Craner RC, Poterack KA. Examining the Burden of Licensure, Certification, and Related Credentialing Costs in Young Physicians. *Mayo Clin Proc*. 2015;90(12):1735-1736.
27. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J Med Syst*. 2018;42(7):130.
28. Liu X, Barenji AV, Li Z, Montreuil B, Huang GQ. Blockchain-based smart tracking and tracing platform for drug supply chain. *Comput Ind Eng*. 2021;161:107669.
29. Pane J, Verhamme KMC, Shrum L, Rebollo I, Sturkenboom MCJM. Blockchain technology applications to postmarket surveillance of medical devices. *Expert Rev Med Devices*. 2020;17(10):1123-1132.
30. Corkery M, Popper N. From Farm to Blockchain: Walmart Tracks Its Lettuce. *The New York Times*. https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html. Published September 24, 2018. Accessed January 26, 2024.
31. Schuchat A. Department of health & human services. *Pharm Today*. 2015;21(11):20-21.
32. Justinia T. Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences. *Acta Inform Med*. 2019;27(4):284-291.
33. Omar IA, Jayaraman R, Salah K, Simsekler MCE, Yaqoob I, Ellahham S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Med Res Methodol*. 2020;20(1):224.
34. Thomson C, Beale R. Is blockchain ready for orthopaedics? A systematic review. *J Clin Orthop Trauma*. 2021;23:101615.
35. Dinov ID. Volume and Value of Big Healthcare Data. *J Med Stat Inform*. 2016;4. doi:10.7243/2053-7662-4-3
36. Pirtle C, Ehrenfeld J. Blockchain for Healthcare: The Next Generation of Medical Records? *J Med Syst*. 2018;42(9):172.
37. Bhavin M, Tanwar S, Sharma N, Tyagi S, Kumar N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *Journal of Information Security and Applications*. 2021;56:102673.
38. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE; 2017:1-5.
39. Wang G, Wang Q, Chen S. Exploring Blockchains Interoperability: A Systematic Survey. *ACM Comput Surv*. 2023;55(13s):1-38.