Blockchain Technology in Healthcare: An Analysis of Strengths, Weaknesses, Opportunities, and Threats

Warren A. Poquiz

Texas State University School of Health Administration

Blockchain Technology in Healthcare: An Analysis of Strengths, Weaknesses, Opportunities, and Threats

EXECUTIVE SUMMARY

The dawn of the ‘crypto’ age has significantly highlighted the potential of Blockchain technology in an array of multi-industry functions. Blockchain challenges existing architecture by offering perhaps one the most efficient, decentralized, and immutable data management platforms ever invented. The inherent characteristics of a Blockchain have been widely regarded by many as a potential solution to current HIT problems. The strengths of Blockchain technology identified in this analysis were interoperability, data accuracy, security, and transparency. Blockchain weaknesses analyzed were lack of standardization, accessibility, ownership, and change management. Several opportunities were identified: revenue cycle management, physician credentialing, electronic health records, and supply chain management. Lastly, the analysis identified the following threats: potential government regulation and internal attacks.

INTRODUCTION

The emergence of cryptocurrencies such as Bitcoin and Ethereum has shined a spotlight on an emerging technology that has the potential to revolutionize the future of financial transactions—Blockchain. According to Ninranjaramurthy et al., a Blockchain is a digitized, decentralized, public ledger utilizing a peer-to-peer approach by linking transactions chronologically to become an immutable chain of information (2018). Blockchain's potential extends far beyond its utilization in the financial industry, this innovative technology has also been tapped to possibly change current logistical approaches in supply chain management (Bencic et. al., 2019; Ahamed et. al, 2020), the government sector (Alketbi et. al, 2020; Bu & Bu, 2020), and agriculture (Vinay et al., 2020). Research on current applications of Blockchain technology in healthcare will be later addressed in this analysis.

Blockchain saw a surge in popularity when it was first introduced with Bitcoin in 2009 by Satoshi Nakamoto. Nakamoto published a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" aiming to combat the problem of double-spending—the act of spending the same amount of digital currency more than once. This phenomenon was highly prevalent in centralized banking institutions wherein banks or other financial institutions serve as the central authority and intermediary between the sender and the receiver. As a response to this threat, Nakamoto developed a peer-to-peer public ledger that eliminates the use of central authority in digital transactions, thereby creating a decentralized system.

Despite being first popularized in 2009, the Blockchain concept was first introduced to the world in the early 1990s. Cryptographer Stuart Haber and physicist Scott Stornetta were concerned about the rapid growth of computer use in American households. Particularly alarmed about the wealth of data stored within the computer and its susceptibility to manipulation, Haber and Stornetta devised the basic underlying structure of a Blockchain— a time-stamped series of ledgers linked together in such a way that one would not be able to tamper with without invalidating the whole chain (Whitaker, 2019). This analysis will aim to examine the strengths, weaknesses, opportunities, and threats of Blockchain implementation in the healthcare industry.

Blockchain Functionalities

As its name suggests, a Blockchain is a chain of interconnected data packages or blocks that contain multiple information (Nofer et al., 2017). Each block contains the data, a timestamp, a hash value, and the hash value of the previous block. In the case of Bitcoin, the data contained within the blocks are transactional information about the sender, receiver, and the transfer amount. As Blockchain technology continues to be utilized in other industries, the information contained within the blocks may vary.

Hashing

Hashing has been one of the most commonly used methods to compress data for fast access and verify information integrity (Chi & Zhu, 2017). The hash value serves as the fingerprint of a block and is utilized to authenticate the block before being added to the chain. The hashing process compresses information of any length (input) and converts it to a random combination of letters and numbers (hash value) using an algorithm (hash function). Hash or hash values are unique and immune to fraudulent attacks as any change in the information contained within the block would immediately change the value of the output (Nofer et al., 2017). Therefore, it is impossible to produce the same hash value using two different inputs. Illustrated below is an example of the hashing process. Using a cryptographic hash function, inputs “Health Information System” and “Health Information System 1” are converted into a hash value consisting of a fixed-length combination of random numbers and letters.

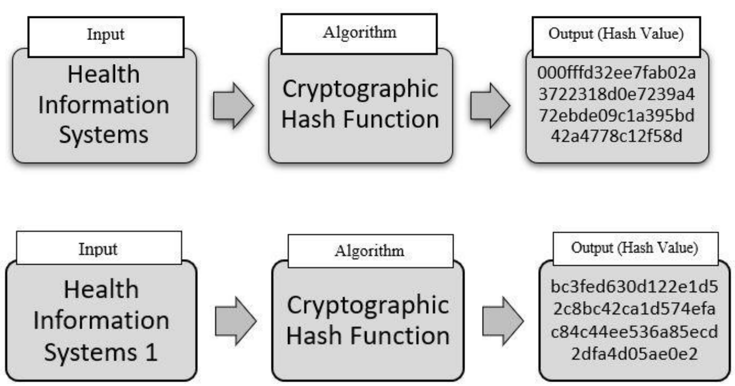

Fig. 1 The hashing process

In a Blockchain, the information contained in the first block, also known as the genesis block, is converted into a hash value. As a second block is generated, the hash value is then combined with all the information contained in the second block to produce a hash value of its own. This mechanism is repeated as subsequent blocks are added onto the chain, thereby creating an almost unbreakable dependency. The hashing process ensures the integrity of the entire Blockchain by linking information back to its genesis block (Nofer et al., 2017).

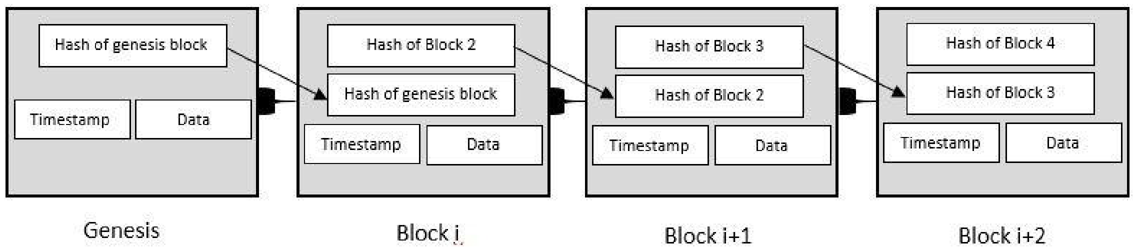

Fig. 2 An example of a Blockchain

Peer-To-Peer (P2P) System and Consensus Mechanism

A prominent feature of Blockchain technology is its decentralized and distributed characteristic. Peer-to-peer networks are utilized in Blockchain to disseminate system information while keeping the system as decentralized as possible without any central authority (Delgado-Segura et al., 2018). Every peer or node within the network contains a copy of the entire chain. Before a block is added onto the chain, a community of peers (computers) agrees on its validity using a consensus mechanism (Nofer et. al, 2017). Consensus mechanisms define the process in which network validators attain a unified agreement on the state of the ledger (Swanson, 2015). A common consensus mechanism used predominantly in Bitcoin is the proof-of-work (PoW). This mechanism slows down the process of creating new blocks by making nodes compete against each other. The competition, which is also called mining, consists of a series of complex calculations on the new block containing unconfirmed data and a hash reference to the previous block (Hölbl, 2018). In Bitcoin's case, the average time to calculate for the required proof-of-work is 10 minutes (Nofer et al., 2017). The first "miner" to offer a solution to the complex mathematical equation will have its answer verified and evaluated by network peers. Afterward, a consensus to either verify or reject the offered solution will be decided based upon a set of rules and procedures. Once a block has been added to the ledger, it can no longer be changed or modified (Nofer et. al, 2017). Proof-of-work is an integral concept of a Blockchain and is one of the many reasons this innovative technology has never had a shortage of hype in the IT world.

Blockchain's hashing process, consensus mechanism, and peer-to-peer system make it one of the most immutable technological platforms ever invented. These built-in security features make it virtually impossible to alter the data inscribed within the distributed ledger. To successfully modify past data, an attacker will have to tamper with every single block in the chain, redo the proof-of-work calculations for each block, and successfully take control of at least 51% of the peer-to-peer network (Nakamoto, 2009).

Types of Blockchain

There are three types of Blockchain technologies depending on the manner in which data will be used, the type of industry, or data availability (Hölbl, 2018).

A public Blockchain (permissionless) is easily accessible to the public. This type of Blockchain is particularly used in cryptocurrencies where anyone is able to participate in the network without the need for approval (Holbl, 2018). However, some portions of the Blockchain are encrypted to maintain the participant's anonymity (Holbl, 2018).

The second type of Blockchain is consortium (public permissioned). This partly decentralized Blockchain enables only a selected number of nodes to participate in the networks (Holbl, 2018). The Blockchain is open for public use and is partly centralized (Holbl, 2018).

Private Blockchains are the most restrictive type of Blockchain. This type of Blockchain only enables certain chosen nodes to join the network, thereby making a distributed yet centralized network (Holbl, 2018). Private Blockchains are permissioned, used only for private purposed, and is managed by one organization also called as the trusted party (Holbl, 2018).

Electronic Health Records

Health Information Systems have drastically evolved within the last two decades. Several initiatives launched to increase the efficiency of patient health information flow, while enhancing interoperability among different healthcare entities, have been at the forefront of the issues facing healthcare IT. Following the great recession that started in late 2007, the United States Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA) which approved a federal government spending of 499 billion dollars for legislative initiatives aimed at modernizing the country's infrastructure (Conley & Dupor, 2013). One of the measures enacted under this legislature was the Health Information Technology for Economic and Clinical Health (HITECH) Act. The initiative provided financial incentives to providers fully implementing EHR systems that are specifically geared towards a meaningful utilization of EHR technology as a way to improve the quality of patient care (Mennemeyer et al., 2015). To ensure EHRs are used properly and in a meaningful manner, the Department of Health and Human Services established the Meaningful Use (MU) Program to set the criteria that providers must meet in order to have a meaningful impact on patient care. The concept of meaningful use is mainly derived from the five pillars of health policy outcomes: quality improvement and reducing health disparities, population health improvement, patient engagement, security and privacy of personal health information (PHIs), and improving care coordination (cdc.gov).

Challenges to Current HIT Models

As the healthcare industry continues to face challenges inherent to the ever-changing field, including patient quality improvement and the efficiency of care delivery, the implementation of proper HIT mechanisms becomes even more critical. Without a systematic health information exchange mechanism between care teams and concerned providers, patient care outcomes can be severely compromised (Esmaeilzadeh & Mirzaei, 2019). The exchange of health information involves the electronic transfer of patient health and medical information among providers and institutions. This process is facilitated by employing two different sharing mechanisms: direct and query-based.

In a direct exchange mechanism, also known as the “push” mechanism, healthcare providers initiate the sharing of patient health information to one another including structured documents such as lab test results, imaging, or ER visits (Vest et al., 2020). This mechanism improves care coordination by incorporating identifiable health information through a secured network controlled by healthcare entities (Esmaeilzadeh & Mirzaei, 2019). Alternatively, a query-based mechanism allows providers to "pull" or request desired information from a shared health information system (Vest et al., 2020). This mechanism allows for the creation of cross-organizational, aggregated, and relevant health records, aiding in both quality improvement initiatives and disease registry development (Esmaeilzadeh & Mirzaei, 2019).

However, despite the significant efforts to improve health information management magnified by the enactment of the HITECH act, health information systems still face an array of challenges concerning data privacy and security, interoperability, and the quality of healthcare outcomes (Durneva & Cousins, 2020). Furthermore, research has also analyzed physician perspectives on EHR implementations and their adverse effects on physician productivity and efficiency (Abramson et al., 2012; Beglaryan, Pterosyan, & Bunker, 2017). The widespread adoption of Blockchain technology among healthcare systems can potentially disrupt and address the challenges of existing HIE mechanisms.

Implementation of Blockchain Technology in Healthcare Systems

Blockchain's built-in features such as immutability, security, decentralized storage, and a distributed ledger make it an ideal platform for health information management (McGhin et al., 2019). Despite being in its infancy, Blockchain technology offers a broad range of potential application within the healthcare industry particularly in the management of electronic health records, revenue cycle management, and system interoperability. This section of the analysis will examine the strengths, weaknesses, opportunities, and threats of Blockchain utilization in healthcare.

Strengths

Security. Hospitals have often been prone to malicious attacks by cybercriminals. Due to its necessity of computer storage of patient care information along with security holes in IT systems, hospitals are an easy target for ransomware attacks (Spence et al, 2018). Ransomware is a type of malware that encrypts digital files in a computer until a sum of money (ransom) is paid (Mansfield-Devine, 2016). In fact, more than 300,000 healthcare data breaches have been reported as of February 2017 (Spence et al., 2018). Additionally, ransomware is responsible for more than a billion dollars in monetary losses every year (Spence et al., 2018). Blockchain implementation could potentially mitigate this problem. Blockchain technology's inherent immutability prevents data breaches as cybercriminals would not only have to control a majority of the nodes within a healthcare Blockchain but also calculate the required proof-of-work on every block that will be tampered with—this is practically impossible given the massive amount of data contained in healthcare systems. Furthermore, Blockchain would not be easily corrupted as its distributed network feature allows for system persistence even if a node has been compromised.

Interoperability. Another strength of a Blockchain-based healthcare system concerns the principle of interoperability. Interoperability involves the transfer of data among different entities (Azaria et. al, 2016). The peer-to-peer Blockchain architecture enables companies to collaborate and share information with other organizations without ceding control (Esmaeilzadeh & Mirzaei, 2019). There are generally two types of interoperability: institution-driven, and patient-driven. According to Gordon and Catalini, institution-driven interoperability concerns the transfer of information among healthcare entities, while patient-driven interoperability concerns the patients' control over their own health records including authorization and releasing information to trusted entities (2018). Blockchain's decentralized and distributed nature, along with its peer-to-peer network system reinforce both interoperability and patient-centeredness.

Transparency. The third strength of a Blockchain platform in healthcare is the transparency of information. System transparency can particularly be helpful in detecting system anomalies. Blockchain's time-stamping mechanism can specifically diagnose what caused the problem within a system as every piece of information in the ledger is time-stamped, thereby making a digital foot-print.

Data Accuracy. Blockchain's cryptographic features and immutability enhance user verification, access control, and security and privacy (Durneva et al., 2020). This authentication feature ensures that the right patient is tied with the right information at all times, thereby minimizing the risk of medical errors.

Weaknesses

Accessibility. Implementing new technology in a healthcare setting requires the support of every single medical stakeholder involved in patient care, including the patient. Patient education on the proper use of personal health records using an entirely new technological platform can be challenging most especially among geriatric patients.

Change Management. Healthcare is a constantly changing environment. Innovative technologies are constantly introduced to achieve a desirable clinical outcome. Widespread implementation of new technology such as Blockchain-based EHRs prompts comprehensive staff training which would take away time from patient care responsibilities. Additionally, HIT-related changes usually involve a shutdown of the current system to facilitate the transition to a new system. This could potentially be detrimental for emergency services and trauma centers as these healthcare institutions function on the provision of prompt and immediate medical care.

Ownership. The decentralized nature of Blockchains offers a myriad of benefits. However, the absence of a central authority increases the possibility of ownership challenges. Legal issues concerning intellectual property rights and compliance would have to be specifically addressed if a centralized liability does not exist.

Lack of standardization. Standardization becomes a concern as more and more industries are looking to employ technology in their operational functions. Blockchain's current lack of standardization due to its relatively immature nature hampers its broad acceptance and slows down development (Olnes, et al., 2017). To enable a widespread propagation of Blockchain technology across different industries, a high level of standardization is needed (Olnes et al., 2017).

Opportunities

Revenue Cycle Management. One of the potential beneficiaries of Blockchain technology is revenue cycle management (RCM). Blockchain can be used to easily correct and verify irregularities with patient information such as demographics, payment information, and insurance policies. The utilization of Blockchain in medical claims processing systems could potentially prevent excessive denials. Furthermore, the use of a Blockchain-based HIT would disintermediate provider-payer relationships and eliminate the use of clearinghouses.

Electronic Health Records. The country of Estonia collaborated with the Blockchain company Guardtime to implement a nationwide EHR using Blockchain technology, thereby allowing its citizens, providers, and insurance companies to retrieve medical information digitally (McGhin, 2019).

Physician Credentialing. Blockchain technology has the potential to assist with the highly complicated and time-consuming physician credentialing process. Utilizing Blockchain with its authenticating features can potentially shorten the recruitment period, avoiding any contracting delays that may result in revenue loss.

Supply Chain Management. Application of Blockchain technology in hospital supply chain management can potentially be very efficient. Research studies reveal the efficiency of Blockchain technology in supply management logistics in other industries (Bencic et. al., 2019; Ahamed et. al, 2020).

Threats

Potential Government Regulation. Blockchain Technology is still in its infancy. Consequently, gaining support from the government is highly unlikely. The question of how a widespread implementation of Blockchain would affect prominent healthcare laws such as HIPAA and HITECH is yet to be determined. However, one potential basis for regulatory measures concerns Blockchain's energy consumption during the mining process. The amount of electricity required to run a large-scale blockchain system is significantly high. In fact, one study found that the Bitcoin network alone consumes the same amount of energy used by certain countries such as Ireland and Austria (de Vries, 2018). The energy burden of Blockchain implementation to manage extremely large data sets in healthcare will particularly receive significant resistance from environmental groups, prompting a potential regulatory action from the government.

Internal Attacks. Despite being immutable, a possibility of internal manipulation exists. Blockchain's immutability relies primarily on the size of the network. Large networks often have more enhanced immutability. However, small Blockchain networks run the risk of 51% attacks—an event wherein a node or group of nodes amasses the majority of the hashing power and alters the chain (mit.edu). In 2018, one of the largest cryptocurrencies at the time, Bitcoin Gold (BTG), suffered a 51% attack that resulted in the alteration of 29 blocks within the chain (Redman, 2018). In addition, more than 7,000 BTGs ($70,000) were double-spent (Redman, 2018). A successful 51% attack on a Blockchain platform in healthcare could have devastating ramifications.

CONCLUSION

This analysis has examined the current state of HIT in healthcare systems. Existing problems with current EHR systems identified were privacy, security, and interoperability. The paper also thoroughly examined the concept of Blockchain structure, the hashing process, and consensus mechanisms. Lastly, the analysis identified the strengths, weaknesses, opportunities, and threats of Blockchain implementation in healthcare. Blockchain's built-in features such as a decentralized system, a peer-to-peer network, cryptographic functions, and immutability make it an ideal platform for the implementation of a national electronic health record system in the United States.

REFERENCES

Abramson, E. L., Patel, V., Malhotra, S., Pfoh, E. R., Nena Osorio, S., Cheriff, A., Cole, C. L., Bunce, A., Ash, J., & Kaushal, R. (2012). Physician experiences transitioning between an older versus newer electronic health record for electronic prescribing. *International Journal of Medical Informatics*, *81*(8), 539-548. https://doi.org/10.1016/j.ijmedinf.2012.02.010

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services—Use cases, security benefits and challenges. *In IEEE 2018 15th Learning and Technology Conference (L&T),* pp. 112-119.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and pemission management. *Researchgate.* 25-30. doi: 10.1109/OBD.2016.11.

Beglaryan, M., Petrosyan, V., & Bunker, E. (2017). Development of a tripolar model of technology acceptance: Hospital-based physicians' perspective on EHR. *International journal of medical informatics*, *102*, 50–61. https://doi.org/10.1016/j.ijmedinf.2017.02.013

Benčić, F., Skocir, P., & Zarko, I. (2019). DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. *IEEE Access*. PP. 1-1. 10.1109/ACCESS.2019.2909170.

Conley, T., Dupor, B. (2013). The american recovery and reinvestment act: Solely a government jobs program?. *Journal of Monetary Economics*, 60(5).

De Vries, A. (2018). Bitcoin's growing energy problem. *CellPress, 2(5),* 801-805. Doi: https://doi.org/10.1016/j.joule.2018.04.016

Delgado-Segura, C. Pérez-Sola, G. Navarro-Arribas, J., & Herrera-Joancomart. (2017). A fair protocol for data trading based on bitcoin transactions. *Fut. Gene. Comput. Syst.* doi: 10.1016/j.future.2017.08.021.

Durneva, P., Cousins, K., & Chen, M. (2020). The current state of research, challenges, and future research directions of blockchain technology in Patient Care: Systematic Review. *Journal of medical Internet research*, *22*(7), e18619. doi: https://doi.org/10.2196/18619.

Esmaeilzadeh, P., & Mirzaei, T. (2019). The Potential of Blockchain Technology for Health Information Exchange: Experimental Study From Patients' Perspectives. *Journal of medical Internet research*, *21*(6), e14184. https://doi.org/10.2196/14184.

Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry*, *10*, 470.

Mansfield-Devine, S. (2016). Open banking: opportunity and danger. *Computer Fraud & Security,* 2016(10). doi: https://doi.org/10.1016/S1361-3723(16)30080-X.

McGhin, T., Choo, K.R., Liu, C., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl., 135*, 62-75.

Mennemeyer, S. T., Menachemi, N., Rahurkar, S., & Ford, E. W. (2016). Impact of the HITECH Act on physicians' adoption of electronic health records. *Journal of the American Medical Informatics Association : JAMIA*, *23*(2), 375–379. https://doi.org/10.1093/jamia/ocv103

MIT Media lab. (n.d.). *51% attacks.* Retrieved from https://dci.mit.edu/51-attacks.

Nakamoto, S (2009). Bitcoin: A p2p2 e-cash system.

Niranjanamurthy, M., Nithya, B., & Jagannatha, S. (2018). Analysis of blockchain technology: pros, cons and SWOT. *Cluster Computing*, 1-15.

Nofer, M. & Gomber, Peter & Hinz, Oliver & Schiereck, Dirk. (2017). Blockchain. Business & Information Systems Engineering. 59. 10.1007/s12599-017-0467-3.

Olnes, S., Ubacht, J., & Jansen, M. (2017). Blockchain in government: Benefits and implication of distributed ledger technology for information sharing. *Elsevier,* 34(3) doi: https://doi.org/10.1016/j.giq.2017.09.007.

Redman, J. (2018). Bitcoin gold attacked- Network loses $70,000 in double spending. *Bitcoin.com.* Retrieved from https://news.bitcoin.com/bitcoin-gold-51-attacked-network-loses-70000-in-double-spends/.

Spence, N., Bhardwa, N, Coustasse, A. (2018). Healthcare facilities: Another target for ransomware attacks. *Management Faculty Research.* Retrieved from: https://mds.marshall.edu/cgi/viewcontent.cgi?article=194&context=mgmt_faculty

Swanson, T. (2015). Consensus as service: brief report on the emrgence of permissioned, distributed ledger systems. *Work Pap.*

Vest, J., Unruh, M., Casalino L., & Shapiro, J. (2020).The complementary nature of query-based and directed health information exchange in primary care practice, *Journal of the American Medical Informatics Association*, 27(1) doi: https://doi.org/10.1093/jamia/ocz134.

Vinay, S., Sing, A. (2019). A systematic review of blockchain technology in agriculture. *Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, Czech Republic, July 23-26, 2019.*

Whitaker, A. 2019. Art and blockchain: a primer, history, and taxonomy of blockchain use cases in the arts. Artivate: *A Journal of Enterprise in the Arts* 8(2), pp.21-47.