

Blockchain Applications in the Healthcare Systems

Posted on January 3, 2024

SECTION 1: INTRODUCTION

Healthcare systems have been developed in the past years with transformations from manual to digital healthcare systems. Digital healthcare systems have paved the way for blockchains which are decentralized data management and transaction systems first developed to accommodate bitcoin cryptocurrency. The blockchain system integrates data and provides anonymity and robust security features without third-party intervention making this system a competitive invention since 2008. Therefore, the features that limit third-party intervention make blockchain a unique tool that prompts research to identify how its application can solve recurrent healthcare data management issues. The healthcare system has often faced challenges due to third-party access to data and the increased data collection of patients, making healthcare facilities and patients lose trust in the existing digital data systems. Blockchain protects user data from manipulation, and its security features foster accountability in acquiring data, processing, and providing results to patients. This paper aims to give an in-depth insight into blockchain applications in healthcare systems.

Problem Statement

Healthcare systems are built on very sensitive data, and who accesses this data is a crucial matter. Healthcare systems often handle complex and sensitive data, which makes it crucial to ensure that every data-handling step is predetermined and appropriately guarded. Therefore, data access and handling are a delicate issue in healthcare facilities as it potentially creates misunderstandings in cases of data mismanagement. Healthcare workers across the globe have often shared their dissatisfaction with the existing data frameworks. This issue has caused some hospitals to witness misdiagnosis, faulty medical procedures, life loss, and wrong procurement of medical supplies. Therefore, introducing blockchain technology in healthcare systems will solve most issues related to tedious data interpretations, mishandling of data, time wastage, and wrongful medical procedures.

Blockchains are categorically divided into private blockchains, public blockchains, hybrid blockchains, and consortium blockchains. Private blockchains are often used in single enterprises to track transactions between individuals or departments. Moreover, public blockchains are fully decentralized systems in which the public can participate in transactions and access content within the blockchain. Besides, consortium blockchains are used in cases where transactions are audited and synchronized to keep track of any exchanges in the system. Consortium blockchains have permitted access to

privileged groups regardless of whether the systems are public or private.

Moreover, hybrid blockchains integrate features of public and private blockchains. Hybrid blockchains employ private blockchains to run in the background to moderate modification access of the ledgers. In contrast, the public blockchain is applied to ensure the ledger is ultimately accessible to the public.

Moreover, blockchain systems will cut costs on the heavy financing to manage and execute medical procedures. Manual and other data management systems require huge financing to pay for human capital, acquire technology and address logistical requirements. The blockchain system meets most of these requirements by creating an autonomous system that requires minimum or no human intervention, thus providing more reliable solutions while minimizing the costs. This technology's major costs are purchases, setup, and maintenance, whereas most intermediaries will be eliminated to reduce operation costs. Moreover, the technology is malware-proof, and this will reduce the employment of software technicians to monitor the system. In addition, there are constant concerns about data synthesis and handling huge healthcare data sets that are tedious to compute and relay. Existing healthcare systems require manual data interpretation and sharing, making the examination and medical processes long and tedious.

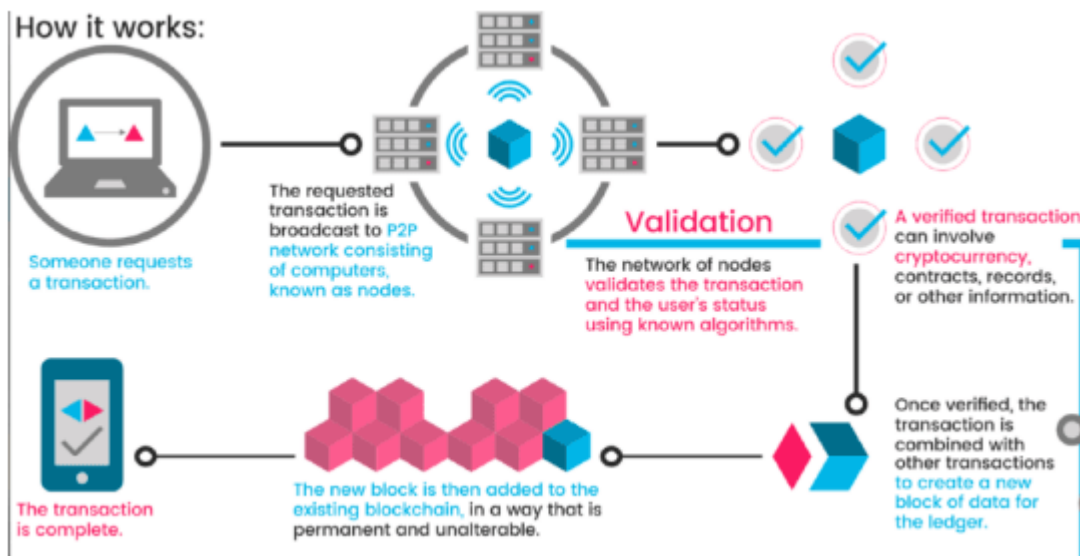


Figure 1: *Sample Blockchain model* (Hameed, 2019)

Blockchain in Healthcare

Blockchain is a promising technology employed in various sectors to overcome security performance issues. This paper introduces a new healthcare model based on blockchain to solve the IOT access in healthcare. The introduction of blockchain in different healthcare systems paved the way for the limitless possibilities, blockchain systems could achieve. Blockchain application has overcome many challenges, including performance, security, and reliability, making it a more competitive digital platform. Introducing blockchains that use network nodes would be a game-changer in ensuring that

healthcare data is safeguarded. The network nodes refer to the computers connected to work in unison and process data with regard to the given commands. The paper introduces a new blockchain model in the healthcare sector that provides fluidity and flexibility in acquiring, processing, and relaying medical data. The model aims to utilize the best blockchain security features and accommodate large datasets to enhance its performance over other models. Moreover, the model aims to reduce some hidden costs when using other models in medical facilities.

SECTION 2: Literature Review

According to research written by Rim, the blockchain is a ledger made up of block sequences that record all transactions executed in the blockchain network (Ben Fekih & Lahami, 2020). The block comprises the header linked by a previous block's hash and a body. The blocks then form chains with each structure based on each previous block. Besides, block headers have timestamps that show the time when specific blocks were published. Moreover, the headers also have a Merkle tree which decreases the required effort to identify transactions in the blocks.

Moreover, the header constitutes a nonce which refers to the numbers frequently changed to get hash values that help solve mathematical puzzles. Blockchains operate under smart contracts that facilitate thorough data processing. The smart contracts are tamper-proof when embedded in blockchains, as the programs cannot be altered. Besides, the blockchains are designed to self-verify and self-enforce due to the automation features that ensure all the requirements are met at all transactional stages. Blockchains can be applied in electronic media records, remote patient monitoring, pharmaceutical supply chain, and health insurance claims.

In another research aimed to show the benefits and threats of blockchain technology, it was reported that blockchains could help in healthcare information exchange, facilitating clinical trials, managing medical insurance, tracking medical supply chains, facilitating system authorization and security, monitoring a patient's health data, personalizing healthcare functions, and monitoring patient's health status (Abu-elezz et al., 2020). The research showed that blockchains boost security features of healthcare systems by placing the patient as a key element in the system while securing the data over peer-to-peer networks. The research emphasizes that the blockchain system is failure proof, and its system requires authentication to verify every time a user tries to access healthcare data under unique identities. Moreover, the study showed that blockchains help physicists easily track patient data through blockchain timestamps. In addition, the research revealed that healthcare providers could share medical records through blockchains which helps develop personalized healthcare plans. Besides, the study also showed that blockchain technology could be impactful in monitoring a patient's recovery journey and taking any emergency action plan in case of any health anomalies.

However, the research also identified significant threats to applying blockchain technology in healthcare systems. The threats include regulation issues, authorization and security concerns, scalability issues, inadequate technical skills, interoperability issues, transaction and installation

issues, social acceptance, high energy demands, and slow processing speeds. The advantages and threats are limited to organizational, technical, and social threats.

Figure 2: Potential blockchain threats in healthcare

Another research aimed to show the application of blockchain technology in facilitating transition patient-driven interoperability, emphasis was put on patient and institution-driven interoperability. Past healthcare systems mostly majored in institution-based interoperability while giving less attention to the patients. Institution-based interoperability mainly operates regulatory and business incentives as healthcare sectors exchange data. However, the digitalization of most healthcare sectors has prompted the need to move away from institution-driven interoperability and focus on patient-driven interoperability. Patient-driven interoperability allows patients to access healthcare data through application programming interfaces. However, patient-centered interoperability attracts challenges like governance, patient engagement, patient consent, security, and privacy.

SECTION 3: Proposed Model

System Model

Imagine having software that maintains a single source of truth where a doctor or any other medical provider can access or request patient information to track the origin of disease or ailment, effectively give prescriptions, and receive payments. The proposed blockchain protects the system's data from unauthorized access by hiding patient identity, enabling them to access healthcare services without fear of a lack of privacy. The blockchain impacts the healthcare industry by creating a telemedicine platform that allows patients to access healthcare services and consultations with doctors via video platforms and pay for consultations through cryptocurrency tokens.

In the first step of the model, data owners have access to the healthcare records and can easily visualize the data as per the system records. The proposed model gives the data owners the right to access their data and other past activities in the blockchain system. Data owners can offer or cancel their consent by prompting the transaction to the smart contracts. In the second step, peer nodes validate the data records and record the exchanges in the designated ledgers. The third step gives the medical officials with the access to the data route to the evaluate data. This third step also allows the data consumers and producers to exchange services and other fees through the cryptocurrency blockchain. The transactions are regulated by smart contracts making them safe from unauthorized access. In the fourth step, the smart contracts access data initially recorded in the blockchain ledgers and verify the authority of the accessing party. The smart contract then validates or invalidates the transaction based on the outcome of the verification process.

The blockchain is a closed and private blockchain that operates on a hyper ledger that manages and allows access to healthcare records. Moreover, the hyper-ledger creates room for scalability and

modularity of the blockchain in case of future expansions. The blockchain has a cryptocurrency form of payment that operates as a smart contract. Therefore, all transactions are verified and recorded on the platform, and the process is automated to ensure smooth transactions. The blockchain system has a two-way, encrypted security system that protects data in transit from malware and unauthorized access.

Figure 3: How the healthcare blockchain model works

Figure 4: Correlation between elements in the blockchain

The blockchain is linked via numerous ledgers limited to healthcare providers or healthcare givers that can access the same data. Consequently, the numerous ledgers create a unique path to ensure that each data set matches the patient and that the path is isolated from third-party access. Moreover, each transaction is recorded on the blockchain to help uphold transparency.

System Component

The proposed blockchain comprises user, storage, and node management. Besides, the blockchain has a client manager that adds, modifies, checks, and overwrites previous orders, similar to deleting the orders. However, since blockchains leave a digital footprint, the blockchain system does not delete previous data but overwrites it. Moreover, the blockchain requires that every block to be verified to ensure that any malicious data or action can be detected and removed from the block. The blockchain has a fixed host; hence, users can easily access and exit the platform. Moreover, the proposed blockchain uses fewer start-up nodes to operate and can easily be used compared to other blockchains.

Consensus Protocol

A consensus protocol of the proposed blockchain refers to the fault-tolerant mechanism that allows system nodes to agree on consistent data over different datasets. The blockchain uses the proof of stake algorithm, which is more efficient, low-cost, and energy-consuming. Moreover, the proof of stake algorithm allocates the nodes with respective ledgers in proportion to the data available on the blockchain. The consensus protocol ensures that the blockchain is efficient despite the constant changes in the status of this blockchain. Therefore, the consensus protocol ensures that all activities follow the rules per the blockchain's design.

Distributed Ledger Technology

Distributed ledger technology refers to the protocols and infrastructure in technology that facilitates successive validation, access, and update of records from different locations, platforms, and entities.

Distributed ledger technology champions for decentralization of the blockchain, unlike traditional platforms that were originally centralized. Distributed ledger technology operates under the cryptography framework, restricting access to cryptographic signatures and special keys. Therefore, data on the distributed ledger technology is immutable and follows specific commands per the blockchain's design. Besides, the peer-to-peer updating and sharing of healthcare records in distributed ledger technology are quicker, cheaper, and more effective than other technologies. Therefore, distributed ledger technology is more tolerant of cyber-attacks.

SECTION 4: System Evaluation

System Security Evaluation

This will entail assessing potential risks to the blockchain and finding ways to curb these problems to ensure that the proposed blockchain is secure. The security will entail the implementation of cybersecurity frameworks, methodologies to test security, and safe coding activities to secure the blockchain from malware, crypto-jacking, and password attacks (Jia, 2021). The security solutions entail: the enabling of identity and access management controls to take care of the data access within the blockchain, securely storing of identity keys, restriction of access to only authorized persons to secure the ledger entries, definition and enforcement agreements based on the health care contacts, use of data classification to secure data or user details, multi-factor authentication, performing vulnerability assessment and penetration testing(VAPT), getting an industry-recognized security certification and also use of strong cryptographic key management(Jia, 2021). Once the system security is in place, ethical hackers and professionals in security will conduct blockchain penetration testing to test the level of security of the blockchain (Kuo et al., 2017). The testing tools include manticore, security 2.0, smart check, octopus, solidity security blog, and the smart contract weakness classification.

Technical Evaluation

Technical evaluation is conducted by the staff or by a specified technical team to determine whether the received offers meet the expectations in the solicitation documents. A mark is given for every criterion evaluated, and the evaluation will take place in the following steps. The scoping and test strategy which the team gains an understanding of the objectives and the technology space and agrees on the basic requirements (Kuo et al., 2017). The test preparation is where the team in healthcare will acquire evaluation products that are required for testing. The test results and final report will be submitted to determine whether the objectives have been met. Finally, the integration and deployment are determined by the blockchain healthcare staff. Each step has different objectives and is associated with executing the task.

Figure 5: Technical evaluation process of the blockchain

The blockchain uses a decentralized ledger that allows each node to access data but only via specified routes. Therefore, the blockchain limits the data to each user hence barring unauthorized access (Agbo et al., 2019). The ledger, through a consensus, maintains its integrity through the different nodes that agree on the real state of the data or process under execution. The blockchain uses cryptography to acquire and execute any preset commands in the blockchain system. The blockchain achieves this by using the public key infrastructure to create and oversee any data exchanges in the blockchain. The parties that have access to the blockchain have a pair of private and public keys to use when accessing the system. The private key is used as a user's authentication pass, whereas the public key is used as the user's public address. Each transaction in the blockchain demands that each step includes the public key at the initiation of the transaction (Agbo et al., 2019). The public key serves as a recipient of the transaction message and transaction, and all characters are cryptographically signed and grouped using the private key. Moreover, the transaction is broadcasted to subsequent nodes in the blockchain network. A block, in this case, is a collection of valid transactions received in the networks and meets the requirements for validation. The validation process counterchecks the authenticity of the data and transaction in the blockchain, ensuring that each transaction is from an authorized user. The authentication process is facilitated by a consensus algorithm that dictates the order in which the authorized are linked to the ledger.

This model has unique nodes that facilitate the running of the consensus algorithms by dictating the order of adding blocks to the network and approving transactions in the blockchain. The system has enhanced security features in which transactions are heavily guarded through upgraded detection (Chauhan, 2022). According to this model, any slight change in the data on the blockchain leads to a drastic change in the corresponding blocks. The drastic change enhances the detection of these alterations, thus making the system more reliable. Consequently, this system ensures that each block is tied to specific chains to ensure that the data on the platform cannot be altered or modified (Frankenfield, 2021). This feature ensures that the data on the platform is fixed and immutable. The function that makes the immutable data demands that a new record must be created on the platform in case of a need to update the data, thus making this healthcare blockchain an append-only ledger. Besides, the limitation ensures that each transaction trail can be audited by an individual user or persons accessing the data.

SECTION 5: Conclusion

In conclusion, introducing blockchain in healthcare is a promising step toward patient-centered service delivery. Besides, blockchain promises robust service provision catering to healthcare facilities as it helps protect data and promote functionality. The blockchain is a positive step towards fluid, reliable and excellent healthcare quality compared to other healthcare systems. However, blockchain application in the healthcare sector still needs to be explored due to the limited research conducted to date. Therefore, much effort must be put into understanding the various blockchain systems and their applicability in the healthcare sector. The discoveries will help ease work in the healthcare sector, improve patient-doctor rapport, hasten healthcare access and protect patient privacy.

Blockchain application remains to be a promising tool in the transformation of the healthcare sector and the development of healthcare solutions.

References

- Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, 142, 104246. <https://doi.org/10.1016/j.ijmedinf.2020.104246>
- Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, 7(2), 56. <https://doi.org/10.3390/healthcare7020056>
- Ben Fekih, R., & Lahami, M. (2020). Application of Blockchain Technology in Healthcare: A Comprehensive Study. *Lecture Notes in Computer Science*, 268–276. https://doi.org/10.1007/978-3-030-51517-1_23
- Chauhan, V. (2022, May 4). *Top Healthcare Blockchain Companies to Watch in 2022*. Blockchain Technology, Mobility, AI and IoT Development Company USA, Canada. <https://www.solulab.com/top-healthcare-blockchain-companies-to-watch-in-2022/>
- Frankenfield, J. (2021, November 30). *Consensus Mechanism (Cryptocurrency)*. Investopedia. <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp#:~:text=A%20consensus%20mechanism%20is%20a>
- Hameed, B. I. (2019). Blockchain and Cryptocurrencies Technology: a survey. *JOIV : International Journal on Informatics Visualization*, 3(4). <https://doi.org/10.30630/joiv.3.4.293>
- Jia, Q. (2021). Research on medical system based on blockchain technology. *Medicine*, 100(16), e25625. <https://doi.org/10.1097/md.00000000000025625>
- Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association : JAMIA*, 24(6), 1211–1220. <https://doi.org/10.1093/jamia/ocx068>
- Qu, J. (2021). Blockchain in medical informatics. *Journal of Industrial Information Integration*, 100258. <https://doi.org/10.1016/j.jii.2021.100258>