Deploying Popular Blockchain Solutions in Healthcare

Aishwarya Pradeep

Undergraduate Student
Computer Science with spec. in Bioinformatics
Vellore Institute of Technology, Vellore, India

***Abstract*: The COVID-19 pandemic has led to a wide spread dire situation, with a lot of uncertainties in how each person is affected and the after-effects of the virus, especially for people with underlying health issues. In such times, it is vital for healthcare providers to understand the patient's entire health history in order to take crucial decisions in terms of treatment or diagnosis, but this is currently challenging due to the massive amount of time required to receive them, or the chances of the data being faulty, or the incompatibility of the records' formats among the organizations, all leading to severe risks in misdiagnosis/wrong treatment of the patients thus increasing medical errors and deaths. Fortunately, there is a potential solution that can overcome all these challenges and yet ensure complete privacy and security - Blockchain technology. Ever since its emergence, it has shown tremendous potential as a viable alternative across multiple domains such as Finance, IoT, Supply Chain etc. While every industry is equally important, the healthcare industry stands out as one of the most essential. This paper aims to explore and understand the diverse solutions recommended to solve the foremost data challenges faced by the healthcare domain and realize the benefits of deploying blockchain specifically for handling patient and medical data.**

***Index Terms*: Blockchain Technology, Distributed leger, Healthcare, Health Records, Hyperledger, IoT, Medical data, Proof-of-Work**

I. INTRODUCTION

Blockchain Technology is a distributed leger technology that is essentially a peer-to-peer network that prioritizes decentralization, immutability, consensus, validation and verification, transparency and higher level of data security. Satoshi Nakamoto, the creator of blockchain originally created it to eliminate the need of a centralized authority in managing transactions and instead be overseen by everyone in a transparent fashion eliminating chances of data corruption. With increase in cyber hacks and database breaches, security has become the need of the hour. Blockchain's popularity lies in its amplified security, decentralized trust and consensus.

According to recent statistics [9], blockchain technology is fast-becoming commonplace, as it is estimated to be valued at $ 15.9 billion by the next three years and at $ 3.1 trillion by the next decade [10]. The success of blockchain technology can be proved with the world-wide popularity of the Bitcoin as a digital currency - its first application.

Research is ongoing in how to best assimilate it into major domains of the world such as global market transactions, education systems, tax payment records etc, while there are several idealistic and speculative proposals, common challenges faced such as implementation difficulties due to funding constraints, architecture set-up etc would need to be addressed prior to large-scale deployment.

II. HISTORY AND DESIGN

Bitcoin run by Blockchain technology, first came into existence in the year 2008, and over the next few years steadily gained attention, from being used to purchase two pizzas, to exceeding the market cap for $1 billion by 2013[11]. Tech giant PayPal also announced its integration to its services in the following year. It gained more momentum, with more developers contributing towards it augmentation with frameworks and platforms like Ethereum, Hyperledger, Multichain, Corda to name a few. With further adaptations by different companies, several types of blockchains came about such as – federated, private, public, hybrid, permissioned and permissionless blockchains. By 2018, several governments have acknowledged the possibility of adapting it in their countries, and in medium to large scale business world-wide and organizations such as Barclays, IBM, CitiBank have developed products and services with blockchain solutions. It has also gained credence from companies such as JPMC and Facebook who aim to make it the technology of the future.

A blockchain, as the name suggests, is quite simply a block of chains connected after following various protocols and algorithms successfully. A block consists of a cryptographic hash, the data to be stored and the hash of the previous block in the chain. The data stores the details of a specific transaction, while the cryptographic hashes are generated by using secure hash algorithms such as SHA-256, Keccak-512 etc, that ensure no two transactions have the same hash value. Any change in the data of the block would lead to changes in the hash value, this in turn prevents tampering of the data.

However, with increasing computational capacity and power, the tampered blocks whose hash values have been changed can easily be recalculated and connected back into the blockchain. In order to prevent the entire blockchain from getting updated- the concept of Proof-of-Work (PoW) was introduced to delay the time required to create a new block. Thus, if one block were to be tinkered with, then the proof of work of all the remaining blocks needs to be recalculated causing major overhead. This is one of many ways blockchain ensures security. Another significant method is to introduce Consensus, wherein a group of anonymous people (nodes) get a copy of the blockchain, such that a new block needs to be validated and verified by all the people in the consensus network in order to be added into the blockchain. Similarly, if any tampering were to be done on a block, the nodes in the consensus would reject the block during the validation process, thus preventing data corruption. Similar to PoW, are the Proof of Stake (PoS) which works to attain consensus by electing the creator of the next block either by random selection or based on age or wealth(stake)

and the practical byzantine fault tolerance protocols that are used in scenarios with larger number of participants and in cases of Byzantine failure.

Based on different circumstances, there are a multitude of blockchain types to choose from. Public blockchain are accessible to anyone wherein the identities and authenticity are unknown but with PoW fraudulent transactions are prevented. Private blockchain is more restrictive than its public counterpart. It is generally employed within organizations with limited participants with complete autonomy in the hands of the deploying organization. Hybrid blockchain as the name suggests, is a hybrid of both public and private blockchain types, wherein certain percentage of the data is maintained in a public blockchain, while the rest are deployed as private blockchains. On the other hand, Consortium blockchains are somewhat less decentralized due to it being managed by multiple organizations.

III. APPLICATIONS

Blockchain applications can be seen in several industries, from the aerospace industries to nuclear reactors. While, blockchain solutions are still not fully integrated, the trend is only growing in coming years. Smart contracts have been the most useful in replacing middlemen dealing in transactions. It enforces accountability and trust. Medical care industries, Banking organizations and FinTech companies have been able to enhance the security of their transactions with lower costs. IoT along with blockchains has been able to significantly boost the security of data consolidated from multiple sources. Fitness apps, Medical sensors and devices are able to maintain patient data preventing data breaches or privacy issues due to blockchain's properties.

The rest of the paper discusses some of the studies made to integrate blockchain technology in handling medical and patient data in the most scalable, affordable and secure manner. The challenges and limitations along with the future of blockchain as a prominent technology especially for the healthcare industry is studied.

IV. BLOCKCHAIN IN HEALTHCARE

Integrating DLT to manage patient health records

Healthcare industry is one of the most data intensive sectors that is confidential and is large in size, requiring tight security lest the data is leaked, corrupted or accessed by unauthorized personnel. When a patient seeks medical attention from an organization different from their usual healthcare provider, the health history is unknown and it would be cumbersome to obtain all the required information from the patient. This problem among others including, use of third-party services due to high cost of maintaining data leading to possible security breaches, use of legacy softwares by different organizations to store patient data would not be compatible with the others' which fuels the need for a unified format and model for health records, privacy concerns of patients and the plausibility of integrating blockchain into healthcare systems are the foremost challenges faced. In an attempt to address them, [1] the study proposes a model- OmniPHR that deploys blockchain technology to store patient records in a protected manner that can be effortlessly maintained and compatible among various health organizations. The model focusses on building a system with a distributed nature that regionalizes and encrypts the data across a network, where multiple parts of a record are scattered to different nodes while maintaining easy and authorized access.

There are many formats for health reports, such as HL7, DICOM, LOINC, openEHR etc, and openEHR format is chosen for its easy interfacing with OmniPHR. The Chord algorithm is preferred due to its ability to balance the network systems, tractability, efficient lookup with complexity of O(log n), and is utilized to search for transactions in a peer-to-peer network. Apart from the source database and depositories, the middleware propositioned consists of a service module that manages the data nodes, validates the blocks before adding to chain, distributes data blocks, router to direct communications, along with a security module that encrypts stored blocks, ensures digital signatures of users for validity, corroborates users to avoid duplicity or corruption and administers privileges accordingly.

It also implements a thorough analysis on the mode's behaviour and performance by exploring possible circumstances in real-time such as observing the results when the system is used by health professionals and using tools like OverSim framework to comprehend the prototype in various states. The analysis shows the merits of deciding on Chord algorithm due to low latency with varying loads but consistent delivery time, and gives significant insights about the potential to augment the model at the same time tackle limitations and challenges that have come by. There is dependency on the patient when it comes to data sharing among different organizations as every access/transaction must be authorized by them leading to overhead, strict enforcement of OpenEHR standard in organizations with legacy systems is difficult that may lead to inconsistent/duplication in patient records and gaining enough confidence so that patients can trust their information to the model can be overcome with deeper investigation. The security of the model should be tested and strengthened due to plausible hacks and decryption by unauthorized users, it also considers integrating a translation unit that can cooperate with various organization yet maintain consistent data effortlessly. The model proposed has a huge potential and further deliberation on how a real-time deployment can be brought closer taking into consideration the factors of feasibility, costs, infrastructure and scalability could revolutionize the industry.

Using Blockchain for secure medical data transaction

Medical data is sensitive and needs to be maintained with utmost precisions. Any duplication, tinkering, technical glitches such as wrong mapping of data to patient, or unauthorized access can lead to severe consequences. This study [2] focuses on the aspects of data privacy especially in the domain of healthcare. Currently, the healthcare industries rely on legacy software consisting of relational or flat structure of databases. The technology used is optimized for maximum efficacy with minimal costs and have been created for convenient sharing and access in a network. This makes it prone to hackers and can lead to a huge breach in the system leading to data leakage and security concerns. The study also explores various endeavours done in this direction specifically security of medical images. It proposes an application that can ensure secure, trusted and valid access to magnetic resonance images or MRI

scans that are critical information of a patient by employing equivalence checking. It converts the medical images into states of automata by finding each image's radiomic attributes, which are then accordingly classified based on their interrelationships.

The methodology of equivalence checking involves two inputs that are checked based on an equivalence relation. The model proposed is inspired from labelled transition systems that can give a multitude of results with varying abstraction levels and corresponding details. There are several equivalence relations known, out of which, weak equivalence is considered as it focusses on finding similarity in behaviours of systems. It ensures the integrity of MRI throughout every transaction by distributed verification. The initial verifications are done by valid sources to ensure the integrity of the MRI. With every equivalence checking done that cross checks the automaton produced with trusted sources, the verified automata are added onto a chain consisting of previously verified ones. Thus, the structural design is likened in blockchain fashion and can be utilized for secure transfer of medical image information.

IoT and Blockchain Technology to manage electronic health records

This study [3] focuses on information access, storage, retrieval in a safe and secure manner which is also convenient to access, especially for IoT based information. With the advent of technology, there have been several gadgets that can be used for monitoring various health statuses of a patient like heart rate monitor, oximeters, sugar levels monitor etc. This leads to an expansion in the volume of patient data involved which is essential for appropriate healthcare that is to be provided. There are a multitude of entities involved in the healthcare domain when it comes to data access and maintenance such as patients, physicians, nurse, other healthcare providers, insurance companies etc. Blockchain is fast becoming a trusted option for high levels of security, and this study proposes a novel approach called pseudonym-based encryption with different authorities to deal with ensuring validity of health records. The multi-layered design of the model provides seamless and reliable functioning of various technological utilities from IoT sensors to Cloud platforms in a blockchain architecture. Elliptic curve cryptography was deployed due to its highly secure nature in the design. An innovative idea to ensure patient privacy and zero tampering of health record, the study came up with a pseudonym-based method to identify patients, ensuring no unauthorized person can gain patient personal information.

The three-tiered model firstly focuses on collecting patient health data from IoT devices such as heart rate monitor etc, and accordingly generates a public and private key for the patient and proceeds to send the information to authenticator and gets stored onto the blockchain along with other necessary attributes such as patient's identification number, previous block's hash, patient's pseudonym etc. This also ensures that data once stored is permanent and cannot be modified by any method. On visiting a healthcare provider, a health record is generated and sent to the cloud, which is then accordingly identified and added onto the specific patient's blockchain after the patient authenticates it successfully once their pseudonym is decrypted with their public key. Thus, the three-tiered system proposed approaches specific challenges in each of its tiers, considering the patient interfacing with the system, the intercommunication among various health organizations and the compatibility of the data shared while ensuring strong security measures throughout any transaction. The model was also validated for the security features it provides with MIRACL tools.

Employing blockchain technology in healthcare applications

With constant improvement in technologies, all domains such as finance, industries, especially healthcare are also revolutionizing. In the current time and age, data privacy has been a major threat and concern. This study proposes using blockchain in healthcare, especially in the management of health records and their access, the main reason being the useful attributes of blockchain technology-decentralized, immutable and reliability. The design of the model involves delegating specific roles to the participants in a blockchain network wherein only those certified by the authority can access the health records. This is done when the user enrols into the service provider and is given a private key and ID. The patient has complete control over who can access their records. Whenever a transaction is added, it is distributed throughout the ledger network ensuring that no modification can be done as there is a timestamp for each transaction made wrt the previous hash.

It also proposes various algorithms for every aspect of the blockchain model such as for the working of the admin, lab technician, clinician and for the patient users. They have also considered the scenario of real-world deployment of their proposal with the help of DLT. As a result, the model developed is well thought-out and has also been evaluated in terms of its performance in multiple scenarios related to resource consumption, size of block data, time required to generate a block, endorsement policies, network traffic, network optimization, transaction access time etc with the help of Hyperledger caliper. Thus, a decentralised system that provides tinker-free, immutable, protected access to the data, while simultaneously supporting fault tolerance and multiple copies of the data across servers was successfully devised. The unique features include the protocols installed for ensures accessibility control giving the patient complete protection of their medical information. Even if one of the nodes in the network were to be disabled or hacked, the system as a whole would not malfunction due to redundant data storage. 75% of the system improved on executing performance optimization along with nearly 50% of latency being reduced.

Medical information exchange via blockchains

Medical data such as drug details, clinical trials etc, if accessed by unauthorized people can have alarming ramifications, making security the foremost concern. This study [5] explores permissioned and non-permissioned blockchain and the scope of their deployment in the medical industry along with the evaluation of consensus algorithm and practical byzantine fault tolerance. It mainly focusses on how to ensure protect and manage data from multiple sensors and monitoring systems of a patient. With changing times, healthcare has become a major industry generating lot of data, data which is sensitive and private, requiring stringent measures to ensures the data can be accessed by only the authorized, is easily retrievable and cannot be tampered by anyone.

A popular choice that can be deployed to achieve this is blockchain technology. It makes use of cryptographic methods such as hashing, along with several consensus policies that ensure sanctioned access. As the entities involved in the healthcare and intensive medicine sector are limited and recognized such as patient, lab technician, surgeon, insurance company, etc. The network of ledgers that store the patient health information can be retrieved easily by a doctor/surgeon to better understand the patient's history and is

crucial in making important decisions. This is especially useful, when the patient has visited multiple healthcare providers, as a result, if not for the record stored in the blockchain, it would make accurate diagnosis of the patient difficult, and it was for this specific aspect that the study proposed a model that uses blockchain to make smarter decisions in intensive medicine.

The model was built on the Hyperledger Fabric platform, and consisted mainly of two ledgers, one to control data corruption- a redundancy ledger and another that monitors the data access, and similar operations- a transaction log ledger. Together along with middleware and database, the architecture promises confidential, incontrovertible and consistent source of patient data management. Many of the applications of blockchain technology such as Smart contracts have proved tremendous potential in ensuring efficient and reliable communication of classified data, thus blockchain solutions once integrated into healthcare can propel the industry into the future.

Transforming Health Information Exchange with Blockchain Solutions

In times of emergencies, patients may visit hospitals different from their usual, this would then require the organization to locate and retrieve the patient's health history from their usual provider, in order to better diagnose and treat them. This can sometimes be delayed due to several issues, some being the time taken to receive the reports, security and privacy issues, varying data/data duplicity etc. The study [6] proposes a model that aims to tackle these challenges using blockchain technology and a system that is centered around the patient. The model consists of deploying a permissioned blockchain that ensures authorized access and two main modules- *Linkage* that is responsible for the entry of the information into the network and priming it for further tasks such as quick retrieval etc, and the other-*Request* for maintaining authorized access and user controls for patients. Patients have complete jurisdiction over who can access their health records, and are maintained separately in a list. The data is encrypted in the blockchain and accessing would require decryption keys warranting sanctioned access. A simulation was conducted based on an original dataset obtained, and was tested with five nodes with several patients and clinicians using it, while a random array of clinicians was selected to access an indiscriminate set of patient records and the time involved in receiving permission, the encrypted data and the decrypting key, along with the number of requests involved was tallied and analysed.

To summarize the process involved, assuming the patient has visited *n* number of the organizations, and say the (n+1)th organization's clinician needs to access the records, then they need to first obtain permissions from the patient which would *allow* them the required privileges, then they would receive *n* separate decryption keys from the *n* facilities, with which they can proceed to access the records from those organizations. The results showed brilliant consistency in the times involved in receiving permissions, the encrypted data with varying number of patient records and organizations, despite fluctuating block generation times.

The challenges faced by the model include the limited scalability realised in terms of the blockchain protocol, as any transactions greater than 13 per second would overload the network leading to a failure, the initial cost and infrastructure required to be setup in each organization would be difficult and a fixed standard of health reports that would be agreed by all the organizations in order to carry out any transaction is essential. With some deliberation and effort, the system can be implemented leading to a more connected and safer world, wherein the patients have complete autonomy over their data and can choose who can and cannot access personal information.

V. CONCLUSION AND PROSPECTS

The foremost challenges observed seems the actual deployment, financial restraints, access regulation, varying staff literacy levels along with IoT-specific, mobile-specific security issues. Additionally, the formats used by various healthcare providers are wide-ranging causing compatibility problems during sharing and communication. By monitoring the patients' health, with a multitude of devices such as heart- rate monitor, sugar-level sensors, emergency prevention for sudden heart attacks, seizures etc and precise diagnostics the patient can receive personalized care from health organizations. Machine Learning can also be arrayed to scrutinize the health data which can further aid in an optimum diagnosis, but the core drawback of this would be the amount of time and training required by the machine to draw smart and plausible conclusions of the data provided. This needs to be further explored and if successful can be of colossal advantage in optimizing the industry.

Blockchain is mainly a peer-to-peer technology that is heavily involved in securing transactions and by engaging it in healthcare where the data involved is enormous and unstructured, it would eliminate the need of third-party service providers between patient and healthcare providers. Moreover, integrating blockchain along with machine learning and IoT as services via mobile health applications can serve as an ideal utility guaranteeing easier patient control over data, along with secure access and patient privacy. Due to the nature of healthcare domain, the data generated per patient is also vast, thus fuelling the need for easy, convenient and protected access with a user-centric system.

There have been some studies conducted on deploying blockchains as a viable solution in healthcare systems in some countries such as the Russian Federation [12]. Their study focusses on replacing the paper archives-based register system to blockchain solutions that are risk-oriented, allowing integration of several other intelligent tools that can support decision making and enhanced security. While, the novelty of blockchain technology is providing highly secure environment for tamper-free transactions, recently there have been numerous security attacks [23], such as on the peer-peer network (Eclipse attack, Sybil attack), mining and Consensus mechanism (51%attack, mining malware, Finney attack), or on smart contract (DAO attack). Nevertheless, the challenges of blockchain technology especially in the field of healthcare is daunting but further research along with appropriate budgeting and time can lead to a safer future.

Table 1 Brief view of popular blockchain solutions

Work Ref.	Novelty	Challenges and limitations	Algorithm and Tools employed
[1]	System that can maintain records by the provider that is always updated, easy to retrieve and share among health providers	Ensuring authentic access to prevent data fraud, despite blockchain's security features. Non-compatibility of health record formats among organizations. Requires further security augmentations	Chord algorithm, openEHR, OMNeT++, Routing overlay, INET
[2]	Applying formal equivalence checking on MRIs by radiomic features	Needs to be validated in real-time scenario. Medical staff need some training to employ it. Low scalability	Equivalence checking, CCS, labelled transition systems
[3]	Multi layered architecture to integrating IoT and blockchain technology	Needs to explore IoT based attacks and how to defend against it.	Internet of Things, ECC, blockchain, MIRACL, PBE-DA
[4]	DLT with symmetric-key cryptography-based access control policy architecture.	Elaborate set-up required, needs to be validated in real-time scenario.	Hyperledger fabric, gRPC protocol, hyperledger composer, smart contracts
[5]	Decision making system deploying blockchain for accurate data used for medical decisions	Requires more training, to increase reliability in supporting clinical decisions	Practical Byzantine Fault Tolerance, Hyperledger Fabric platform, SQL/ NoSQL
[6]	Permissioned blockchain that gives patient complete autonomy	Difficult initial setup in various organization. Limited scalability due to Ethereum constraints. Non-compatibility of health record formats among organizations	Smart contract, Ethereum, Surveillance, Epidemiology, and End Results dataset[20]

REFERENCES

[1] Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. Journal of biomedical informatics, 71, 70-81.

[2] Brunese, L., Mercaldo, F., Reginelli, A., & Santone, A. (2019). A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods. Procedia Computer Science, 159, 1787-1794.

[3] Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier blockchain framework for IoT-EHRs systems. Procedia Computer Science, 141, 159-166.

[4] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.

[5] Guimarães, T., Silva, H., Peixoto, H., & Santos, M. (2020). Modular Blockchain Implementation in Intensive Medicine. Procedia Computer Science, 170, 1059-1064.

[6] Zhuang, Y., Sheets, L., Chen, Y. W., Shae, Z., Tsai, J. J., & Shyu, C. R. (2020). A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. IEEE Journal of Biomedical and Health Informatics.

[7] Clim, A., Zota, R. D., & Constantinescu, R. (2019). Data exchanges based on blockchain in m-Health applications. Procedia Computer Science, 160, 281-288.

[8] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh and W. Hong, "Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward," in IEEE Access, vol. 8, pp. 474-488, 2020, doi: 10.1109/ACCESS.2019.2961372.

[9] https://www.statista.com/topics/5122/blockchain/#:~:text=Worldwide%20spending%20on%20blockchain%20solutions,estimated%2015.9%20billion%20by%202023.&text=Around%2066%20percent%20of%20global,the%20experimentation%20or%20deployment%20stage.

[10] https://101blockchains.com/history-of-blockchain-timeline/

[11] https://builtin.com/blockchain

[12] Koshechkin, K. A., Klimenko, G. S., Ryabkov, I. V., & Kozhin, P. B. (2018). Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation. Procedia Computer Science, 126, 1323-1328.

[13] Zhang, Y., Wen, J., 2017. The iot electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications 10, 983–994.

[14] S. Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, (2008)

[15] An overview of blockchain technology: architecture, consensus, and future trends, in: Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang (Eds.), Big Data (BigData Congress), 2017 IEEE International Congress on, IEEE, 2017.

[16] B. Reeder, A. David, Health at hand: a systematic review of smart watch uses for health and wellness, J. Biomed. Inform. 63 (2016) 269–276.

[17] S. Safavi, Z. Shukur, Conceptual privacy framework for health information on wearable device, PloS One 9 (12) (2014) e114306.

[18] M. del Rosario, S. Redmond and N. Lovell, "Tracking the Evolution of Smartphone Sensing for Monitoring Human Movement", Sensors, vol. 15, no. 8, 2015.

[19] J.E. Han, M. Rabinovich, P. Abraham, P. Satyanarayana, T.V. Liao, T.N. Udoji, G.A. Cotsonis, E.G. Honig, G.S. Martin, Effect of electronic health record implementation in critical care on survival and medication errors, Am. J. Med. Sci. 351 (6) (2016) 576–581.

[20] D. National Cancer Institute, Surveillance Research Program. Surveillance, Epidemiology, and End Results (SEER) Program Research Data (1975-2016).

[21] BlocHIE: a BLOCkchain-based platform for healthcare information Exchange, in: J. Shan, C. Jiannong, W. Hanqing, Y. Yanni, M. Mingyu, H. Jianfei (Eds.), 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 18-20 June 2018, Los Alamitos, CA, USA: IEEE Computer Society, 2018.

[22] Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for healthcare 4.0 environment: opportunities and challenges. Comput Electric Eng 2018;72:1–13.

[23] https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

[24] Sun Y, Zhang R, Wang X, Gao K, Liu L. A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th International conference on computer communication and networks (ICCCN); 2018. p. 1–9.

[25] Frost & Sullivan, Global Blockchain Technology Market in the Healthcare Industry 2018–2022, (2019) 4847375

[26] S.A. Anastasia Theodouli, K. Moschou, K. Votis, D. Tzovaras, On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing, (2018).

[27] T. Nugent, D. Upton, M. Cimpoesu, Improving data transparency in clinical trials using blockchain smart contracts, F1000 Res. (2016) 5.

[28] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, et al., Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare, Oncotarget 9 (5) (2018) 5665–5690.

[29] Xu,X.,Weber,I.,Staples,M.,2019.Blockchainpatterns,in:ArchitectureforBlockchainApplications.Springer,pp.113–148.

[30] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where is current research on blockchain technology?a systematic review. PloS one 11, e0163477.

[31] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, J. Liu, S. Qing, D. Liu, C. Mitchell, L. Chen (Eds.), Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems, Springer Verlag, 2018, pp. 387–398.

[32] P. Zhang, D. Schmidt, J. White and G. Lenz, "Blockchain Technology Use Cases in Healthcare", Advances in Computers, p. 32, 2018.

[33] L. Linn and M. Koo, "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research", ONC/NIST Use of Blockchain for Healthcare and Research Workshop, 2016

[34] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When intrusion detection meets blockchain technology: A review", IEEE Access, vol. 6, pp. 10179-10188, 2018.

[35] F. Casino, T. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status classification and open issues", Telematics Inform., vol. 36, pp. 55-81, Mar. 2018.

[36] B. Reeder, A. David, Health at hand: a systematic review of smart watch uses for health and wellness, J. Biomed. Inform. 63 (2016) 269–276.

[37] C. Esposito, A. Castiglione, F. Palmieri, Interoperable access control by means of a semantic approach, in: 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 2016, pp. 280–285.

[38] T. Wang, D. Dolezel, Usability of Web-Based Personal Health Records: An Analysis of Consumers' Perspectives, Perspectives in Health Information Management 13 (Spring).

[39] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.

[40] T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller (Eds.), Blockchains Everywhere – A Use- Case of Blockchains in the Pharma Supply-Chain, Institute of Electrical and Electronics Engineers Inc, 2017.

[41] Boulos, M. N. K., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.

[42] Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. JMIR mHealth and uHealth, 5(7), e111.

[43] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, B. Ford, OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. IEEE Symp. Secur. Priv., 583–598 (2018)

[44] Skiba, D. J. (2017). The potential of blockchain in education and health care. Nursing education perspectives, 38(4), 220-221.

[45] Casado-Vara, R., & Corchado, J. (2019). Distributed e-health wide-world accounting ledger via blockchain. Journal of Intelligent & Fuzzy Systems, 36(3), 2381-2386.

[46] Jo, B. W., Khan, R. M. A., & Lee, Y. S. (2018). Hybrid blockchain and internet-of-things network for underground structure health monitoring. Sensors, 18(12), 4268.

[47] Funk, E., Riddell, J., Ankel, F., & Cabrera, D. (2018). Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Academic Medicine, 93(12), 1791-1794.

[48] Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to use blockchain for diabetes health care data and access management: an operational concept. Journal of diabetes science and technology, 13(2), 248-253.

[49] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

[50] Amofa, S., Sifah, E. B., Kwame, O. B., Abla, S., Xia, Q., Gee, J. C., & Gao, J. (2018, September). A blockchain-based architecture framework for secure sharing of personal health data. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6). IEEE.

[51] Gropper, A. (2016, August). Powering the physician-patient relationship with hie of one blockchain health it. In ONC/NIST use of Blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST.