IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW ON DECENTRALIZATION IN HEALTHCARE SYTEMS USING BLOCKCHAIN

[1]Atharv Kulkarni, [2]Lalkrishna Joshi, [3]Yukta More, [4]Anjali Mudaliar, [5]Prof. Deptii Chaudhari

[1]Student, [2] Student, [3]Student, [4]Student, [5]Assistant Professor

[1]Dept. of Computer Engineering,

[1]International Institute of Information Technology, Hinjawadi Pune, India

Abstract: The exchange and use of healthcare data are controlled by hospitals and not patients. With features such as immutability, availability, confidentiality, unique identification, provenance and decentralized management, Blockchain can drive significant changes in existing data exchange and ownership models by shifting the system to a patient-centered model. The substantial increase in the adoption of sensors and IoT devices has allowed us to propose systems for monitoring health in real-time; moreover, the system would send an alert message to patients and concerned medical authorities if some anomaly is detected. In this study, we explore the benefits of blockchain in maintaining and sharing electronic health records (EHRs), seeking insurance, and securing the exchange of IoT data between patients and health facilities. Scalability is a fundamental issue of the blockchain. Hence, we also explore off-chain data stores for storing patient information and history, EHRs, and information related to insurance and insurance claims in this article. We also provide a comprehensive analysis of studies used to Analyse IoT data for heart attacks and to reduce the time it takes to diagnose.

Keywords **- Blockchain, IoT, AI, Healthcare.**

I. INTRODUCTION

Blockchain is good at keeping track over time due to its immutable and decentralized design that is ensured by a peer-to-peer network. Previous and current generations of blockchain deal with smart properties and contracts. They also allow keeping track of assets by embedding the details in the metadata of the transaction in the block. The next generation of Blockchain will solve the fundamental problems with previous generations of Blockchain, like scalability and interoperability, and see its mainstream adoption in various fields like healthcare, gaming, decentralized finance (DeFi), supply chain management, etc. In this survey, we shed light on the applications of blockchain technology and how it can be used alongside technologies like IoT and AI, in the healthcare sector.

Data ownership is a crucial challenge in healthcare; the patients have no control over their medical data. Healthcare institutes control the access to medical data of patients. Electronic Health Records (EHRs) are scattered across various hospitals, thus making it difficult to maintain a long-term medical history. It also affects the privacy of patient data when EHRs are stolen or hacked from the hospitals [40]. Health Centers can use Blockchain to securely store and share medical data while ensuring that only patients have complete access to their medical records [19]. It would help the health Centers protect users against data leaks [17] and solve integrity-related problems, thereby building a patient-centric model [18].

Healthcare has also seen a significant rise in the application of IoT devices and sensors to record medical data. All the IoT devices used for recording medical data generate a vast amount of data at a very high speed. Technologies used for tracking the level of the saline bottles [21], real-time cardiovascular data [12] [20] assist in accurate diagnosis and monitoring of the patient's health. The readings obtained from the sensors are more reliable than the symptoms mentioned by the patient, as there's almost no human intervention involved. The data collected from the sensors can be processed and then shared with the patient and the concerned medical authorities for further analysis to reduce the time taken for prediction [7] of probable diseases.

II. LITERATURE REVIEW

Maintaining up-to-date medical records of a patient is a difficult task especially when data is distributed among various independent centralized entities who might not share patient data for political, financial or other reasons. Storing information in a centralized system poses problems like a single point of failure, trust, integrity, interoperability, security and privacy.

To reduce collusion and tampering of the IoT ecosystem and build trust between parties and devices, it is essential to access the IoT devices and store IoT data safely and securely. Several factors like piracy, device failure can lead to the generation of corrupted data by IoT devices.

Blockchain stores a part of IoT generated data. Although blockchain can be used for incommutable data, it cannot detect corrupted data. Therefore, testing IoT devices is crucial before integration. Protocols such as CoAP and MQTT can help protect the communication of data.

Health-related data collected from IoT sensors and medical devices can be utilized to provide better monitoring services to users. In remote health monitoring systems, data security and accuracy are the major concerns that need attention.

Different insurance companies can define their own format and process for claiming insurances. This creates a problem of interoperability. Fraudulent documents can be shared by the insured party. Pharmaceutical fraud, such as changing manufacturing dates, cannot be detected without a good provenance system.

We explore and address the solutions to the aforementioned problems in our survey below.

A. *Electronic Health Records*

To fulfil the concept of data ownership, Liang et al. [1] propose a user-centric health data sharing solution that uses Hyperledger fabric [11] to develop a permissioned blockchain and implements privacy channels for private data sharing. By implementing access control policies, the patient is in control of his/her medical data and its sharing with respective medical authorities. They use the cloud database as the off-chain storage and store the proof of integrity in the form of Merkle root on the blockchain. Authors perform testing on the generation and validation of the data integrity proof and conclude that the system can handle a large dataset at low latency.

Azaria et al. [24] developed MedRec, a decentralized record management system to handle Electronic Health Records. MedRec includes a cryptographic hash of the record on the blockchain to ensure that the record has not been tampered with. Since every transaction is recorded in the blockchain, healthcare authorities have accountability for each request and update of the data. With the help of Ethereum smart contracts, a relationship between patients and healthcare authorities is created that determines the viewing permissions and data retrieval instructions from an external database.

Off-chain storage is necessary to overcome the problem with the storage of large files on the blockchain. Steichen et al. [2] present a solution to securely store and access the data stored on the IPFS network. It proposes to store the actual file on IPFS and store the IPFS file hash on the blockchain. Access control is not an inbuilt feature with IPFS so the paper proposes to use Ethereum smart contracts to maintain a dynamic access control list and develops a modified IPFS system, acl-IPFS, that can enforce this access control list. Decentralized and secure storage and sharing framework was developed by Wang et al. [25] where they use IPFS, Ethereum blockchain and attribute-based encryption to achieve fine-grained access control over data.

TABLE I Features of existing EHR Systems

Reference	**EHR Systems**	**User Interface**	**Framework**	**Blockchain Type**	**Algorithm**	**Off-chain Storage type**
[33]	Medi Bloc	Web App	Panacea	public	Delegated Proof of Stake, Practical Byzantine Fault Tolerance	undefined

[34]	Medical Chain	Web API	Hyperledger Fabric	Permission-based	Hashing Algorithm	Not defined
[35]	MedRec	Not defined	Ethereum	public	Proof of Work	Off-chain database
[39]	Medi Chain	Web App	Hyperledger	private	undefined	cloud
[36]	Patientory	Mobile App	Ethereum	Not defined	PTOYMatrix	Not defined

B. Secure Exchange and Management of IoT Data with Blockchain

IoT devices are introducing the need to manage identities at an exponential rate. Identity Management is essential in the IoT ecosystem for its scalability, security, and privacy. Addressing these issues [39] proposed a lightweight architecture for consortium blockchain-based identity management in IoT. To address the scalability issue, the proposed design consists of separating functions of identity management, such as registration, revocation, and authentication into three separate ledgers. The three ledgers can communicate and share information privately to execute simultaneous transactions. The architecture is implemented using a Hyperledger fabric framework and the work mainly discusses the advantages of using a private blockchain instead of using a public one to solve these issues in IoT.

To access the IoT devices safely and to securely store and retrieve the data, [3] and [5] proposed a way to integrate the Hyperledger Fabric and IoT devices. For integration, an attribute-based access control (ABAC) mechanism is created using Hyperledger Fabric components to gain access to the IoT devices. Fabric-iot [3] uses Access Contract (AC): a program to implement access control methods for normal users, Device Contract (DC): a way to store the URL of resource data produced by devices, Policy Contract (PC): a way to manage ABAC policies for admin users. The IoT device used in [5] is Raspberry Pi 4 Model B, they are getting about 200 TPS on reading temperature function and the system has an average latency of 0.27s. Proposed systems in [3] and [5] can provide dynamic, fine-grained, and decentralized access control management in IoT.

Oumaima Attia, Ines Khoufi, Anis Laouiti, Cédric Adjih [4] propose an architecture that ensures secure remote monitoring using IoT and precisely monitors patient-connected devices and retrieves their collected data in the blockchain. The proposed architecture consists of a Blockchain named “medical devices Blockchain” to satisfy these requirements. The sensors are in charge of collecting data that will be stored in the medical devices Blockchain. The data stored in the Medical Devices Blockchain is retrieved from the patient sensors with the NDN (naming data networking) paradigm. This means data is fetched with its name instead of using the device's IP addresses, the paper states this method accommodates well for intermittent connectivity and mobility.

C. Insurance Claims

L. Zhou, L. Wang, and Y. Sun [13] proposed a blockchain-based medical insurance storage system called MI Store (Medical Insurance Store), Idea behind the system is that the insurance company should be able to know the sum of a patient's specific spending records without learning anything about them, otherwise it may result in information leakage. The few important features of the systems are 1) Decentralization 2) Secure data storage: The System uses practical byzantine Fault-tolerance (PBFT) as its consensus mechanism. Therefore, data that has been included by nodes in the blockchain cannot be modified 3) Verifiable: The patient may verify whether his spending data is correctly processed by the hospital and insurance companies. Also, the insurance company can verify whether responses are correctly computed or not. MI Store uses Ethereum as the blockchain platform, Ethereum's block contains transactions of at most 62,360 bytes, and its transaction payload contains at most 1014-byte data, so the MI Store's efficiency is limited because of these factors, therefore if we use some other appropriate blockchain we may get better throughput.

D. Remote Healthcare Monitoring and Prediction for Heart Disease

[26] presented a mobile application based on IoT and ML for the prediction of heart attacks. The data is continuously collected from multiple sensors and sent to the application via a Bluetooth module. Data analysis is done on this data for plotting the status of health and diagnosis of heart disease. An alert system is added for emergency notification. This system eliminates human intervention.

The systems proposed in [6] and [7] are trained with the UCI repository dataset, and machine learning classification algorithms for detecting the presence of heart abnormalities by analyzing the data collected from IoT biosensors. KNN and J48 gave the best accuracy, respectively. To keep an eye on cardiac patients, the authors of [14] proposed an android application that continuously fetches certain physical attributes through the IoT wearable sensors to keep an eye on cardiac patients. This application is built with Blynk [27], which processes the collected data and sends the notification of all details to family and doctors if the calculated value exceeds the preset value.

The cost-efficient and low-power system proposed in [8] collects important cardiac attributes through IoT sensors and sends them to the cloud database. The smartphone application analyzes data with signal processing, and these details are forwarded to concerned authorities through an alert system. By integrating AI, IoT, and Cloud [12] proposed a framework where required data collected from biosensors is directly saved on Cloud. It detects and tracks heart attacks by visualizing data for users and sending alerts on the LCD.

[16] sends alert messages for drop or rise of heart rate from pre-set value with Arduino board. [10] contains the information on machine learning algorithms for data analysis of physiological data recorded from various biosensors. [9] proposes a system that monitors heartbeats, sends warning messages to the physician when the heartbeat rises or falls below a preset level, locates the patient in an emergency. [15] presents 'k-Healthcare', providing efficient storage, fetching, and analysis of the sensor data and using the four layers together. The various sensors are in the Sensor layer; communication of data happens via the Network layer; the Internet layer handles management and storage of data; the Service layer grants access to patients and medical authorities.

The main features of the health monitoring systems proposed and developed in the research papers studied above are summarized in Table II and can be referred below.

TABLE II Features of monitoring system in literature survey

Reference	Use of Machine Learning	Signal Processing	Storage with Cloud Technology	Android Application for User Interface	Emergency alert system	Use of IoT Sensors	LCD Display For Alerts
[7]	✔		✔			✔	
[9]			✔		✔	✔	
[10]	✔					✔	
[12]	✔	✔	✔	✔	✔	✔	✔
[16]		✔			✔	✔	✔
[26]	✔	✔	✔	✔	✔	✔	

E. Supply Chain Management Through Blockchain in Healthcare

The safety and integrity of medical data, patient's identity, and transactions can be ensured by blockchain in the healthcare sector. Effective supply chain management (SCM) has always been challenging. Hence, SCM in healthcare is riskier as it can directly affect the patient's health. Hence, the integration of blockchain and SCM can help us overcome this challenge and produce effective outcomes without risking privacy and security. Threats like grey markets, falsified drugs (also known as counterfeiting) are involved in pharmaceutical SCM that has resulted in a higher mortality rate [32] [29].

Throughout the process of delivery of drugs, the ownership is changed which has led to counterfeiting of the drug. Thus, there's an essential need of securing the procedure to avoid fatal consequences in the healthcare area.

[28] has proposed an approach for a reliable transfer of ownership and traceability of drugs using blockchain. The process begins with erecting a trusted network in which the data could be saved on a permissioned blockchain which is then followed by verification of the originality.

According to [29] Russia has been one of the leading transactional locales that have recorded the most range of counterfeiting of medicines. As a result, they came up with a pharmaceutical SCM model grounded on Hyperledger Fabric [11]. One of the pivotal features of this paper is the involvement of the government at some stage in the procedure to ensure smooth administration of networks and enrollment of new medicines.

[30] has enforced a blockchain-grounded pharma supply chain. They've integrated IoT as well to record the temperature and other medical data which will be stored in a relational database. Servers have been introduced for communication between blockchain and frontend users to store data in the database and create smart contracts. [31] is similar to the papers mentioned above except for the database used. In this model, e-prescription along with dose and information of the patient is stored and shared using permissioned blockchain. Smart contracts are enforced for the data consistency of drug and health-related data.

[32] has constructed a med ledger fabric blockchain platform for counterfeiting and traceability of medicines. Using this Med ledger, stakeholders gain access to immutable information without the intervention of any central authority. Patients or any stakeholders are given a unique drug code and consignment number after completion of registration through a mobile app, that can be used to explore the source of the drug and transfer history. Moreover, using this model every stakeholder can track and trace the products. Shipments and deliveries along with the location of transactions. Like all the papers mentioned above, [33] has also tried minimizing counterfeiting by establishing evidence of power. RFID tags can be cloned easily, hence it's high time we use blockchain to secure the process pharma SCM. According to this paper, a new transaction will be pushed into the blockchain every time the ownership changes. They've also compared Ethereum and Hyperledger Fabric [11] along with many disadvantages of using blockchain-grounded pharma supply chain.

Ethereum and Hyperledger Fabric were the frameworks used in all the proposed models for Supply chain management. Table III summarizes the technologies and platforms used in all the papers mentioned in this section, thereby helping us understand the correspondence between the methodologies used.

TABLE III Summary of the survey on supply chain management

Paper	Framework	Off-chain storage	User Interface	Type of Blockchain	Smart contracts
[28]	Ethereum	Distributed ledger	Mobile app	permissioned	yes
[29]	Hyperledger Fabric	undefined	undefined	permissioned	yes
[30]	Ethereum	PostgreSQL	Mobile app	undefined	yes
[31]	Hyperledger Fabric	undefined	undefined	permissioned	yes
[32]	Hyperledger Fabric	CouchDB	web-app	permissioned	yes
[33]	Hyperledger Fabric	undefined	undefined	permissioned	yes

III. DISCUSSION

It is possible to use Blockchain to take out a centralized authority and exchange data in a completely trustless environment. The data to be exchanged is included in the metadata of the peer-to-peer transaction. Blockchain can address problems with user data like interoperability, privacy, security, data ownership and reliability.

Scalability is a critical bottleneck in the blockchain and the slow consensus is responsible for limiting the number of successful transactions per second. For comparison, transactions per second (TPS) carried out by Visa is 1667 TPS while Ethereum and Bitcoin carry out 20 TPS and 4 TPS, respectively [41]. Proposals like a lightning network [42] and Eth2 [43] to increase the number of transactions performed per second by Bitcoin and Ethereum blockchain respectively seem promising.

Although scalability remains a big challenge in blockchain, maintaining EHRs while having access control over them is possible. Sharing and storing large files like X-rays, CT and MRI scans, et cetera on the blockchain is inefficient as they will be replicated on each node in the network. This will also adversely affect transaction speed as it would take more time to complete the consensus and then replicate the data over to all nodes. To overcome these problems, the amount of data stored on the chain should be as small as possible. Huge files can be stored and handled by off-chain solutions.

IoT devices produce a huge amount of personal data. Securely exchanging and utilizing this IoT data can be achieved by using blockchain. Blockchain can solve problems with unique identification of devices, privacy and reliability of the personal IoT data. Patients are free to give access to their data to healthcare authorities and can further be used as a means for remote health monitoring and prediction of various diseases.

Fraud detection would be much more efficient with the use of blockchain technology. Insurance companies and patients have access to public information and can quickly verify the integrity of the decision and insurance claim. Patients can track the provenance of various medical equipment and medicines through this immutable distributed ledger thus, reducing the cost to find pharmaceutical frauds and detecting counterfeit drugs.

IV. CONCLUSION

This paper presents an analysis about how the blockchain can foster decentralized healthcare systems. We also presented a review of the state-of-the-art, and an evaluation of relevant literature and challenges for that subject. We composed and reviewed topic related literature and blockchain projects to describe the current state of the work. Due to the limited literature, and the number of products in concept or model status, we noticed that the usage of blockchains in healthcare is in an early development stage. Nevertheless, the blockchain technology along with IoT can make valuable contributions to the healthcare domain, for example, by improving interoperability, privacy, security, data ownership and reliability aspects of healthcare infrastructure. Altogether, after our review, we summarize that the capabilities of the blockchain technology for healthcare are by far not exploited to its potential yet. We conclude that the decentralized blockchain can have a significant positive impact in the healthcare domain depending on the technology's acceptance by the associated stakeholders.

REFERENCES

[1] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361.

[2] Steichen, Mathis & Fiz Pontiveros, Beltran & Norvill, Robert & Shbair, Wazen & State, Radu. (2018). Blockchain-Based, Decentralized Access Control for IPFS. 10.1109/Cybermatics_2018.2018.00253.

[3] H. Liu, D. Han, and D. Li, "Fabric-iot: a Blockchain Based Access Control System in IoT," 2020, p. 12.

[4] Oumaima Attia, Ines Khoufi, Anis Laouiti, Cédric Adjih. An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. NTMS 2019 - 10th IFIP International Conference on New Technologies, Mobility and Security, Jun 2019, Canary Islands, Spain. pp.1-5,ff10.1109/NTMS.2019.8763849ff. Ffhal-02434834f.

[5] Iftekhar, A.; Xiaohui, C.;Tao, Q.; Zheng, C. Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications. Entropy 2021, 23, 1054.https://doi.org/10.3390/e23081054.

[6] A. Gupta, S. Yadav, S. Shahid and V. U., "HeartCare: IoT Based Heart Disease Prediction System," 2019 International Conference on Information Technology (ICIT), 2019, pp. 88-93, doi: 10.1109/ICIT48102.2019.00022.

[7] M. Ganesan and N. Sivakumar, "IoT based heart disease prediction and diagnosis model for healthcare using machine learning models," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 2019, pp. 1-5, doi: 10.1109/ICSCAN.2019.8878850.

[8] Raut S; Vahora S, Shah V, Ranka R(2021).IoT Based Real Time Heart Health Monitoring System. 2021 International Research Journal of Engineering and Technology (IRJET).

[9] TV Sethuraman, Kartik Singh Rathore, Amritha G, Kanimozhi G, IoT based system for Heart Rate Monitoring and Heart Attack Detection, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019.

[10] Vashistha, R., Dangi, A.K., Kumar, A. et al. Futuristic biosensors for cardiac health care: an artificial intelligence approach. 3 Biotech 8, 358 (2018). https://doi.org/10.1007/s13205-018-1368-y.

[11] Androulaki, Elli & Barger, Artem & Bortnikov, Vita & Cachin, Christian & Christidis, Konstantinos & Caro, Angelo & Enyeart, David & Ferris, Christopher & Laventman, Gennady & Manevich, Yacov & Muralidharan, Srinivasan & Murthy, Chet & Nguyen, Binh & Sethi, Manish & Singh, Gari & Smith, Keith & Sorniotti, Alessandro & Stathakopoulou, Chrysoula & Vukolic, Marko & Yellick, Jason. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.

[12] Wan, J., A. A. H. Al-awlaqi, M., Li, M. et al. Wearable IoT enabled real-time health monitoring system. J Wireless Com Network 2018, 298 (2018). https://doi.org/10.1186/s13638-018-1308-x

[13] L. Zhou, L. Wang, and Y. Sun, "MIStore: a Blockchain-Based Medical Insurance Storage System," 2018, p. 17.

[14] Taştan, Mehmet. (2018). IoT Based Wearable Smart Health Monitoring System. Celal Bayar Üniversitesi Fen Bilimleri Dergisi. 343-350. 10.18466/cbayarfbe.451076.

[15] K. Ullah, M. A. Shah and S. Zhang, "Effective ways to use Internet of Things in the field of medical and smart health care," 2016 International Conference on Intelligent Systems Engineering (ICISE), 2016, pp. 372-379, doi: 10.1109/INTELSE.2016.7475151.

[16] Nikunj Patel,Princekumar Patel,Nehal Patel. Heart Attack Detection and Heart rate Monitoring Using IoTInternational Journal of Innovations & Advancement in Computer ScienceIJIACSISSN 2347
–8616Volume 7, Issue 4April 2018.

[17] G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184, doi: 10.1109/SPW.2015.27.

[18] Chen, H. S., Jarrell, J. T., Carpenter, K. A., Cohen, D. S., & Huang,
X. (2019). Blockchain in Healthcare: A Patient-Centered Model. Biomedical journal of scientific & technical research, 20(3), 15017–15022.

[19] J. Liu, X. Li, L. Ye, H. Zhang, X. Du and M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647713.

[20] Eka Adi Prasetyo Joko Prawiro, Chun-I Yeh, Nai-Kuan Chou, Ming-Wei Lee, Yuan-Hsiang Lin, "Integrated Wearable System for Monitoring Heart Rate and Step during Physical Activity", Mobile Information Systems, vol. 2016, Article ID 6850168, 10 pages, 2016. https://doi.org/10.1155/2016/6850168

[21] Sayli Zende, Avinash Devare, Tanvi Kulkarni, Shubhada Yadav, Ajay Biradar, Live tracking of saline for betterment of patient, International Journal of Reconfigurable and Embedded Systems (IJRES), ISSN: 2089-4864, DOI: 10.11591/ijres.v9.i3.pp178-182.

[22] Priti Tagde, Sandeep Tagde, Tanima Bhattacharya, Pooja Tagde, Hitesh Chopra, Rokeya Akter, Deepak Kaushik, and Md. Habibur Rahman, Blockchain and artificial intelligence technology in e-Health, doi: 10.1007/s11356-021-16223-0

[23] Ed-daoudy, A., Maalmi, K. A new Internet of Things architecture for real-time prediction of various diseases using machine learning on big data environment. J Big Data 6, 104 (2019). https://doi.org/10.1186/s40537-019-0271-7

[24] Azaria, Asaph & Ekblaw, Ariel & Vieira, Thiago & Lippman, Andrew. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 25-30. 10.1109/OBD.2016.11.

[25] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," in IEEE Access, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[26] AKM Jahangir Alam Majumder, Yosuf Amr ElSaadany, Roger Young, Donald R. Ucci, "An Energy Efficient Wearable Smart IoT System to Predict Cardiac Arrest", Advances in Human-Computer Interaction, vol. 2019, Article ID 1507465, 21 pages, 2019. https://doi.org/10.1155/2019/1507465

[27] https://blynk.io/

[28] Haq, Ijazul and Olivier Muselemu. "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs." International Journal of Computer Applications 180 (2018): 8-12.

[29] Bryatov, S R and Aleksandr A. Borodinov. "Blockchain technology in the pharmaceutical supply chain: researching a business model based on Hyperledger Fabric." Information Technology and Nanotechnology (2019).

[30] T. Bocek, B. B. Rodrigues, T. Strasser and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 772-777, doi: 10.23919/INM.2017.7987376.

[31] Uddin M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. Int J Pharm. 2021 Mar 15;597:120235. doi: 10.1016/j.ijpharm.2021.120235. Epub 2021 Feb 4. PMID: 33549813.

[32] Jamil, Faisal, Lei Hang, KyuHyung Kim, and DoHyeun Kim. 2019. "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital" Electronics 8, no. 5: 505. https://doi.org/10.3390/electronics8050505

[33] R. Raj, N. Rai and S. Agarwal, "Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 1572-1577, doi: 10.1109/TENCON.2019.8929271.

[34] Medibloc. https://medibloc.com/ (Accessed 30 November 2021).

[35] Medicalchain, 2018. https://medicalchain.com/ (Accessed 30 November 2021).

[36] MedRec, 2016. https://medrec.media.mit.edu/ (Accessed 30 November 2021).

[37] Patientory. https://patientory.com/ (Accessed 30 November 2021).

[38] Rouhani, Sara & Butterworth, Luke & Simmons, Adam & Humphery, Darryl & Deters, Ralph. (2019). MediChainTM: A Secure Decentralized Medical Data Asset Management System. 10.1109/Cybermatics_2018.2018.00258.

[39] Mohammed Amine, Bouras & Lu, Qinghua & Dhelim, Sahraoui & Ning, Huansheng. (2021). A Lightweight Blockchain-Based IoT Identity Management Approach. Future Internet. 13. 24. 10.3390/fi13020024.

[40] Koczkodaj WW, Masiak J, Mazurek M, Strzałka D, Zabrodskii PF. Massive Health Record Breaches Evidenced by the Office for Civil Rights Data. Iran J Public Health. 2019;48(2):278-288.

[41] Mechkaroska, Daniela & Dimitrova, Vesna & Popovska-Mitrovikj, Aleksandra. (2018). Analysis of the Possibilities for Improvement of BlockChain Technology. 1-4. 10.1109/TELFOR.2018.8612034.

[42] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." (2016).

[43] Ethereum, https://ethereum.org/en/eth2/ (Accessed 30 November 2021