

A Research on impact of Blockchain in Healthcare

Padmavathi. U, Narendran Rajagopalan

Abstract—Blockchain refers to a distributed ledger technology that represents an innovation in recording and sharing information without the need for a trusted third party. Blockchain technology offers new tools for security and privacy concerns. Marching towards digitization and analytics, this technology emerges as a promising solution for authentication and authorization issues. It sounds so amazing that this technology that originated with cryptocurrencies could not only be applied in digital contracts, financial and public records, and property ownership but also in medicine, education, science and so on. The use case of this technology springs up in every possible direction. This article first analyses the need for this breakthrough technology and explains how this technology works. This work presents a review on various types of blockchain, the consensus mechanisms used, their advantages and limitations. It provides an overview on the various use cases of this technology. This work mainly focuses on its application in Healthcare. The goal of this article is to analyze the usage of Blockchain technology in various fields of Healthcare such as Electronic Health Record, Health Insurance, Biomedical Research, Drug Supply, Medical Education, Remote Patient Monitoring, Interoperability, Location Sharing etc., It investigates the current research trends and finds the gaps and limitations of these approaches. Moreover, it proposes some enhancements to fill in the gaps in the present approach. This work also analyses the importance of Wearable Internet of Things (IoT) devices in HealthCare and the integration of these devices with Blockchain. Finally, this work concludes by comparing Blockchain 3.0 with previous versions.

Keywords: BlockChain, Healthcare, IoT, authorization, authentication, security, cryptography

I. INTRODUCTION

Blockchain originally called Block Chain, is a distributed ledger technology, which was developed by Satoshi Nakamoto in 2008, as the public ledger of the cryptocurrency bitcoin. The term blockchain which could be called backbone of the transport layer of Internet, is defined as decentralized, distributed, immutable digital ledger which is used to record transactions across many computers in a peer to peer network. Blockchain could be called as a database, where the data is located in a network of computers with no central authority controlling the data. Blockchain is a combination of brainstorming technologies applied in a promising way. It makes use of cryptographic techniques that provides authentication and authorization.

Blockchain promises to be an outstanding solution for

Revised Version Manuscript Received on July 18, 2019.

Padmavathi. U, Department of Computer Science and Engineering, National Institute of Technology Puducherry, Karaikal, Tamilnadu, India.
(Email: udayarajepadma@gmail.com)

Narendran Rajagopalan, Department of Computer Science and Engineering, National Institute of Technology Puducherry, Karaikal, Tamilnadu, India. (Email: narendran@nitpy.ac.in)

many problems in various fields. This technology started to

spring up in many fields including medicine, science, education, food supply chain management, power grid, asset management and so on. This paper first discusses about the need for this technology and the way it works. This paper focuses on the need of this ever growing technology in healthcare. The main goal of this article is to review the application of this technology in various fields of medicine. This work finds out the gap and tries to fill the gap by giving simple solutions.

The following are some of the motivating factors for using the Blockchain Technology :

1. No need to depend on huge servers.
2. Reduce the need for more trusted parties
3. Reduces redundant work
4. Cost effective and fast.
5. Provides security, integrity and privacy of data

The motivating factor for the application of Blockchain in Healthcare

Healthcare presents the most sensitive data. Digitization helps to move the records on paper to digital format which could be easy to store and record. This digitized healthcare data is called as Electronic Health Record. It becomes inevitable to share, access and analyse the health records which in turn facilitates the healthcare providers to access all the medical data of a patient as well as reduces the burden of patients carrying a bundle of papers on hand during their visits to the providers. Eventhough these records provide more benefits, there are certain things that must be taken into account. This sensitive data are the prime target for cyber attacks for financial gain.

The critical policies and technical components required for nationwide interoperability defined by Office of the National Coordinator for Health Information Technology cannot be addressed by the current technologies, since they have security, privacy and interoperability limitations. [1]

Blockchain Technology which is robust against attacks and failures can be the solution for the above issues. Blockchain technology provides a good framework for health care data. It acts as a barrier for tampering and security breaches of healthcare data. The use of this brainstorming technology in healthcare reveals integrity of Personal Health Information and clinical research results, unchangeable medical audits, reduces complexity and expenses, ensures data safety and regulatory compliance, enables trustless collaboration and creates secure and immutable information.



II. TYPES OF BLOCKCHAIN

Blockchain is of three types. They are

- Public
- Private
- Federated or Consortium

2.1 Public Blockchain

A disruptive technology, based on Proof of Work(PoW) Consensus algorithm in which anyone can join the network at any time and can do transactions. In this type of Blockchain, the transactions are transparent, that is the transactions are known to everyone in the network. Anyone in the network can audit the blockchain. This type of Blockchain is Permissionless and opensource. Public Blockchain is employed in BitCoin, Ethereum, litecoin, Monro, Dash and Dodgecoin.

2.2 Private Blockchain

Private Blockchains are permissioned blockchains in which only the organization that owns the Blockchain can run full node and make transactions. The security of the private blockchain depends upon the honesty of the entity validating the transaction. This kind of blockchain is faster and more trusted than permissionless blockchain. This type of blockchain could be employed in places where high confidentiality, privacy and control are required. Multichain and Bankchain are examples of this type of blockchain.

2.3 Federated Blockchain

Federated or Consortium Blockchain are semi-permissioned blockchain in which a consortium of members are responsible to run a full node and make transactions. This blockchain provides more scalability and higher transaction privacy. Only selected members can review or audit transactions. R3, EWF, B3i, Corda makes use of this type of blockchain.

The flowing table summarizes the differences between types of blockchain:

Parameters	Public	Private	Federated
Type	Permissionless	Permissioned	Semi-permissioned
Network	Decentralized	Partially decentralized	Hybrid between public and private
Access	Anyone, Anywhere	Single entity control	Set of nodes control
Speed	Slower	Faster	Moderate
Example	Bitcoin, Ethereum	Bankchain, Multichain	R3, Corda

III. CONSENSUS

Consensus is defined as the set of rules or a fault tolerant mechanism used in blockchain system to ensure all transactions occurring on the network are genuine and all participants agree on a single value or a single state of the network among multi-agent systems. There are different kinds of consensus mechanisms used in Blockchain system[2]. They are as follows.

1. Proof of Work
2. Proof of Stake
3. Delegated Proof of Stake
4. Proof of Elapsed Time

5. Proof of Authority
6. Proof of Capacity
7. Proof of Burn

3.1 Proof of Work

Miners add a block to the Blockchain by solving cryptographic puzzles. Immense amount of energy and computational usage is needed for this purpose. When a miner solves the puzzle, blocks are given to the network for verification[3]. After verification, blocks are added to the blockchain. The limitation associated with this consensus mechanism is it uses sheer amount of power and energy. It is vulnerable to 51% attack. Bitcoin makes use of this consensus mechanism.

3.2 Proof of Stake

In this, miners are replaced by validators. Some of the coins of validators are locked up as stake. The validators then start validating the blocks. The blocks could only be added to the chain only if the validators place a bet on it. Upon successful completion of block being appended, a reward proportionate to their bets will be given to the validators. The major drawback in this type of consensus is that chain splits could occur.

3.3 Delegated Proof of Stake

It is an efficient variant of Proof of Stake in which transactions are validated and the blockchain is maintained by “delegates” selected by the coin holders. The coin holders make use of voting mechanism to select their delegates. This type of consensus mechanism saves energy and promotes decentralization but the drawback lies in achieving sufficient decentralization.

3.4 Proof of Elapsed Time

This is a type of consensus mechanism in which a random waiting time is being created by a number of nodes in the network. In this mechanism, blocks are added to the blockchain by the node with the smallest waiting time. With this, the round gets finished and the process is repeated. In each round, a new block is created and appended to the blockchain. It is similar to Proof of Work but it does not involve mining activity. It consumes less power than PoW.

3.5 Proof of Authority

It is an optimized Proof of Stake consensus mechanism developed as a solution to the problem encountered by Ethereum’s Ropsten test network. This mechanism leverages identity and reputation count in the form of stake rather than monetary value. It requires less computational power than PoW model.

3.6 Proof of Capacity

In this type of consensus, solutions are computed and stored on the hard disk of the computer even before the mining begins. The mining devices make use of these



solutions and add new blocks to the blockchain. It could also be called as proof of space, since it relies on huge amount of storage space than on computing power. DoS attack prevention and anti-spam measures make use of this consensus mechanism.

3.7 Proof of Burn

It works by allowing the miners to burn or destroy the currencies by sending it to the unspendable addresses. It is more efficient than PoW. It could be thought of as long term commitment for a project that users probably accept. The limitation here is it only makes rich people richer and a positive outcome cannot be guaranteed.

IV. APPLICATIONS OF BLOCKCHAIN IN VARIOUS FIELDS OF HEALTHCARE

4.1 Patient driven interoperability

[4] Proposed a blockchain technology that facilitates patient driven interoperability through five mechanisms such as digital access rules, data aggregation, data liquidity, patient identity and data immutability. The challenges associated with patient driven interoperability such as patient consent, governance, security, privacy and patient engagement are addressed by the use of blockchain technology. The limitations associated with this method are scalability, incentivizing interoperability, issues around patient key management and patient engagement.

4.2 Electronic health record

[5] Demonstrates the feasibility of using acceleration data like solution supported by deep learning algorithms. It proposes a blockchain based on IOTA capable of sharing anonymous patient related tremor data helping to consolidate the research. The utility of blockchain in our context is to provide trust and common understanding of data without dependencies from a central authority or specific hardware. IOTA allows implementing cost free transactions with easier trust scheme.

[6] Presents FHIRChain, an architecture based on blockchain designed to satisfy ONC(Office of the National Coordinator for Health Information Technology) requirements. It demonstrates the collaborative decision making for remote cancer care using FHIRChain based dapp(Decentralised Application). The advantages provided by this approach include increased modularity, scalable data integrity, fine grained access control and enhanced trust. The challenges that this approach faces is it does not address semantic interoperability. Moreover, the proposed system is not compatible with legacy systems not supporting FHIR. The cost involved in the development of dapp must also be taken into account.

[7] Demonstrates the opportunities for the use of blockchain in healthcare. With the help of Blockchain, patient medical records could be managed easily. There is no need for the patient to carry out bunch of papers containing their medical history and diagnostic procedure results with them every time they visit a health care provider. Moreover, the use of blockchain technology could reduce storage costs, boost efficiency, decrease the need for manual documentation

processing, lower or prevent the potential for fraud, corruption. This work concludes that utilization of blockchain has its own weaknesses. Currently, the technology is under development and is extremely immature and lacks public or even expert knowledge, thus making it hard to have a clear strategic vision of its potential future uses.

[8] Proposes a secure electronic health record system based on attribute based cryptosystem and blockchain technology. This work uses combined AB/IB-ES primitive to achieve the different functions of ABE, IBE and IBS in one cryptosystem to facilitate management of system and also avoids the need to introduce different cryptographic systems for different security requirements. The blockchain technology is used to ensure the integrity and traceability of medical data. This approach avoids the possibility of a single institution being controlled or bribed to record the accounts. The data on the blockchain is traceable, and also cannot be tampered with.

[9] Proposes a novel blockchain based data preservation system for medical data. This work makes use of proof of possession of primitiveness of data to preserve the characteristics of data in blockchain. Blockchain based data preservation system is implemented on Ethereum platform. Compared to general electronic data preservation system, the proposed work addresses the issues of easy loss or tampering of data or farfetched data. The challenge with this approach is that the cost for storing increases as the size of the data increases. Moreover, long data will lead to transaction failure and the response time increases as the number and size of concurrent transaction increases.

[10] Proposes a blockchain based information management system MeDBlock to handle patients information. The proposed work guarantees user's privacy contained in his data by utilizing the combination of access control and encryption technology. Hybrid consensus mechanism is used to avoid unnecessary waste of resources and to achieve green communication. The proposed system is compared with other existing systems which show that MedBlock is outstanding in privacy and security. But, the limitation here is data congestion caused on uploading data in real time.

[11] Studies the potential use of blockchain technology to protect Health care data hosted within the cloud. It describes the practical challenges that are associated with this proposition. The major advantage of utilizing blockchain eliminates the need for mediator, patients have control over their data. Moreover, Medical history of patients could be achieved in an efficient, verifiable and permanent way. The property of immutability could be taken both as advantage as well as disadvantage. The problem in this proposition is blockchain could store only transaction data that is relatively small in size and linear.

[12] Presents a blockchain based platform consisting of NEM multisignature blockchain contracts for sharing healthcare data. Multisignature contracts refer to the requirement of more than one key to authorize a transaction to the blockchain. The major advantage of this work is patient



can set access permissions and designate who can read and write healthcare data to the account. The limitations of this approach are immutability and this work does not discuss what data are to be stored on the blockchain and what data are not to be stored on the blockchain.

[13] Proposes MeDshare a blockchain based system that addresses medical data sharing issues and provides data provenance, auditing and control of data in cloud repositories among big data entities. This system makes use of smart contracts and access control mechanisms to effectively track the behavior of data and revoke access to offending entities on detection of violation of permission on data. The limitation of this approach is that latency increases as the number of request per cloud service provider increases.

4.3 Biomedical research

[14]presents a notarization service based on blockchain. It employs smart digital contracts to seal a biomedical database query and the respective results. The goal is to ensure data integrity and non-repudiation. Result of this work show that a blockchain based database query notarization service is viable and can support additional functionalities such as versioning of retrieved results over time. The limitation is that there is a tradeoff between the complexity of the supported operations and the cost of the corresponding transactions.

4.4 Remote patient monitoring

[15] Proposes blockchain based smart contract to facilitate secure analysis and management of medical sensors. This system provides real time patient monitoring by sending notifications to patients and medical professionals. It also supports medical interventions. It resolves many security vulnerabilities associated with remote patient monitoring and automates the delivery of notifications to all involved parties in a HIPAA compliant manner. The disadvantage of this proposed approach is that data from smart devices to blockchain nodes is transmitted over an open channel. Moreover, this approach could not be used in emergency conditions as there is a minor delay for block verification times which could increase response times

4.5 Drug supply chain

According to WHO, the term counterfeit drugs can be defined as “Products deliberately and fraudulently produced and/or mislabeled with respect to identity and/or source to make it appear to be a genuine product”.

The World Health Organization (WHO) estimates counterfeit pharmaceuticals lead to more than 1 million deaths annually and can cause severe adverse reactions. Given the potential for falsified pharmaceuticals to enter the supply chain, it’s imperative pharmacists and patients gain transparency into where medicines originate and if they’ve been tampered with, replaced, modified, or stolen.

Pharmacists also need to ensure medicines have been stored correctly throughout their journey and contain the correct quantity and strength of the drug. Responsibility for providing such assurances often falls on manufacturers or wholesalers, resulting in limited visibility for the pharmacist and patient.

[16]Along with the inherent health risks associated with

taking counterfeit pharmaceuticals, the potential for falsified medicines to enter the supply chain and lack of visibility into product quality and authenticity can cause a patient to feel he/she can’t confidently take their medicine, which also drives detrimental health effects.

To overcome the above issues, [17]applies Gcoin Blockchain’s double spending prevention mechanism. In this, transaction data is given to the drug receivers directly by the manufacturers and this data is recorded in the Gcoin Blockchain. This in turn helps to find the invalid transaction if an illegal distributor tries to send counterfeit drugs. Moreover, Gcoin helps to shift the surveillance from the hands of government to all participants who are involved in the network.

[18]gives an insight into how blockchain is used in modum.io for the pharmaceutical supply chain. Modum.io is a startup that uses IoT sensor devices to record temperature of pharmaceutical products during its transport. The advantage of this approach is that it guarantees data integrity due to the deployment of blockchain. Modum.io does not discuss about the counterfeit of drugs during manufacturing process.

4.6 Insurance

[19]proposes a medical insurance storage system based on blockchain. This system consists of record nodes and light nodes. Record nodes used to store entire Blockchain list employs Practical Byzantine Fault Tolerance(PBFT) to maintain the Blockchain and light nodes store only the Block headers. This system employs ECDSA, ECIES and SHA-256, which could not be violated. In this system, the transactions are first verified and then appended to the Blockchain network which helps the insurance company to save the time wasted in verifying transactions.

V. IMPORTANCE OF WEARABLE IOT DEVICES IN HEALTHCARE

[20]Internet of Things(IoT) can be defined as a system of interrelated computing devices forming a giant network of connected things and people capable of transferring data over a network. The word “things” in IoT refers to any device for which an IP address can be assigned and is capable of transferring data over a network. For example, a person with heart monitor implant, an automobile that has built-in sensors, a farm animal with a biochip transponder are called as Internet of Things.

Nowadays, IoT devices are being used by organizations in a variety of industries to operate more efficiently, to understand customers, to deliver enhanced customer service, improve decision-making and increase the value of the business.

[21] Wearable devices also called as wearables are smart electronic devices that are incorporated into clothing or worn on the body as implants or accessories. These devices collect data from human body and transfer it over network using short range Bluetooth or local Wifi setups. Wearable devices could be smart watch, fitness trackers, Activity trackers, Google



glass and so on. These devices are best examples of IoT devices.

To improve efficiency and to lower operational costs, the healthcare industry is ready to make use of connected medical devices. Wearable IoT devices help in remote monitoring of patients vital signs and health statistics. With the help of these devices, healthcare providers and patients stay connected which in turn helps the patient to get control over their health status and to get immediate treatment in case of emergencies.

Forbes in its prediction says that [22] 87 percent of health care organization will have adopted IoT technologies by 2019.

Wearable IoT devices play a vital role in healthcare and the use of these devices in healthcare includes the following:

1. Wearable devices are used to monitor fitness, health and wellness factors.
2. Acts as health care indicator on a day-to-day basis.
3. Helps the patient to share their medical data with the healthcare providers.
4. Helps consumers to motivate themselves for a healthier living.

Although IoT and wearables are considered a boon for the healthcare industry, there are certain challenges such as privacy, security should be addressed. As most of the data is being moved to the cloud, it is easy for private and sensitive data to fall into the wrong hands.

VI. INTEGRATION OF IOT WITH BLOCKCHAIN

Since the smart devices in IOT are always lightweight and have less energy and memory, blockchain cannot be applied directly. [23] proposes a blockchain model based on hyper graphs which could be applied to smart homes and can facilitate maintaining security and privacy protection requirements. The major advantage of this approach is the scope of the attack, is greatly reduced. Some of the challenges remain such as construction of linearly independent matrix needs effective algorithm, accuracy of attack detection needs to be studied.

[24]A survey is conducted in which different application areas of IOT devices are considered and the available literature is organized. Two usage patterns such as device manipulation and data management are presented. The study found that there are two primary necessities such as a solution needs to be developed to grant data privacy and data integrity and a system must be designed that is able to manage the unique identity of devices in a tamper proof manner. The findings of the study reveal that a lot of research has to be done in specific domains like smart energy and smart manufacturing. It also found that only very little research has been done to address the scalability of blockchain solutions. In future, the research could be carried out to protect against side channel attacks and also how blockchain could be applied to solve the problem of exchange and trading.

[25] delineates an agile softwarized infrastructure for smart Health Care applications and services deploying IoT. It analyses the role of data and decision fusion which shows that data fusion provides more accurate result consuming more powerful sensor networks as compared to decision fusion which gives less accurate result consuming constrained power

of the sensors. In this work, analytics is being done on data stored on the cloud that helps to improve healthcare delivery and reduces operational and capital expenditure. The privacy of the healthcare data is preserved using Tor which is deployed in between fog and cloud nodes. The security of the data is guaranteed using Blockchain. Major advantages associated with this method include seamless data aggregation, accurate data management, low cost softwarized IoT, less resource consumption. On the downside, softwarized IoT requires integration of 5G systems. Moreover, all the transactions on Blockchain is visible to all which must be overcome by employing secure communication protocols on the members of the Blockchain or in between individual IoT devices.

VII. BLOCKCHAIN 3.0 & RESULTS

Blockchain 3.0, the current version of blockchain is based on Directed Acyclic Graph(DAG) and comes as a solution to many of the problems faced by the previous versions of Blockchain. This fascinating technology has its birth a decade ago. The first generation of Blockchain called Bitcoin(2008) is originally designed for cryptocurrencies. Over time, the second generation of Blockchain came into existence with the birth of Ethereum and smart contracts in the year 2014. These two versions differ from each other in many ways. One among them is the way, the consensus is reached. Blockchain 1.0 makes use of Proof of Work whereas Blockchain 2.0 makes use of Proof of Stake. Some limitations that are associated with these versions such as scalability, interoperability, sustainability, privacy and governance. These problems are addressed in the next generation, Blockchain 3.0 which is under development. Blockchain 3.0, whose underlying technology DAG works according to horizontal scheme whereas the previous on vertical scheme. A comparison on the various versions of Blockchain is given in the following table.

Attributes/Blockchain version	Version 1.0 (Bitcoin)	Version 2.0 (Ethereum)	Version 3.0 (IOTA)
Mining	Miners	Miners	Each node
Speed	7 TPS	15 to 20 TPS	Increases as the number of nodes increases.
Language	Stack based	Turing Complete	Turing Complete
Hashing Technique	SHA-256	Ethash	Curl
Reason	Created as an alternative to regular money	Is developed as a platform which facilitates peer-to-peer contract applications	Is designed as a communication protocol for IoT
Data Structure	Linked List	Linked list	DAG
Block validation time	10 minutes	14 to 15 seconds	No blocks
Vulnerability	Vulnerable to brute force attacks and quantum computers	Vulnerable to quantum computers	Quantum resistant



VIII. CONCLUSION

The present study gives a perspective on the status quo of Blockchain in Healthcare. This tantalizing technology offers a radical new way towards privacy and security. The exponential growth of this technology proves its lingering features. This work shows that much of the potential of blockchain technology is concentrated towards sharing Electronic Health Records. Other areas such as biomedical research, drug supply chain, insurance needs to be considered by blockchain researchers. Furthermore, it is also found that none of the research paper discloses the indepth details of Blockchain implementation. Even though, blockchain technology offers promising features, there are certain setbacks such as scalability, flexibility, and governance. These features can be scope for research in the future work.

REFERENCES

1. "Blockchain: Opportunities for health care | Deloitte US." [Online]. Available: <https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html>. [Accessed: 05-Dec-2018].
2. "Types of Blockchains & DLTs (Distributed Ledger Technologies)." [Online]. Available: <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/>. [Accessed: 03-Jan-2019].
3. "Basic Primer: Blockchain Consensus Protocol - Blockgeeks." [Online]. Available: <https://blockgeeks.com/guides/blockchain-consensus/>. [Accessed: 04-Jan-2019].
4. W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, 2018.
5. X. Zheng, A. Vieira, S. L. Marcos, Y. Aladro, and J. Ordieres-Meré, "Activity-aware essential tremor evaluation using deep learning method based on acceleration data," *Park. Relat. Disord.*, 2018.
6. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.
7. I. Radanović and R. Likić, "Opportunities for Use of Blockchain Technology in Medicine," *Appl. Health Econ. Health Policy*, 2018.
8. H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," *J. Med. Syst.*, vol. 42, no. 8, 2018.
9. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-Based Data Preservation System for Medical Data," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, 2018.
10. K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–11, 2018.
11. C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, 2018.
12. S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, "How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept," *J. Diabetes Sci. Technol.*, p. 193229681879028, 2018.
13. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain," *IEEE*

Access, vol. 5, no. c, pp. 14757–14767, 2017.

14. A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval," *Comput. Struct. Biotechnol. J.*, p. #pagerange#, 2018.
15. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, 2018.
16. "Blockchain and the Pharmaceutical Supply Chain: Driving Security and Transparency | AWS Partner Network (APN) Blog." [Online]. Available: <https://aws.amazon.com/blogs/apn/blockchain-and-the-pharmaceutical-supply-chain-driving-security-and-transparency/>. [Accessed: 05-Dec-2018].
17. J. H. Tseng, Y. C. Liao, B. Chong, and S. W. Liao, "Governance on the drug supply chain via gcoin blockchain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, 2018.
18. 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 Symp. Integr. Netw. Serv. Manag.*, pp. 772–777, 2017.
19. L. Zhou, L. Wang, and Y. Sun, "MISStore: a Blockchain-Based Medical Insurance Storage System," *J. Med. Syst.*, vol. 42, no. 8, 2018.
20. "What is internet of things (IoT)? - Definition from WhatIs.com." [Online]. Available: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>. [Accessed: 05-Dec-2018].
21. "What is a Wearable Device? - Definition from Techopedia." [Online]. Available: <https://www.techopedia.com/definition/31206/wearable-device>. [Accessed: 05-Dec-2018].
22. "Five IoT Predictions For 2019." [Online]. Available: <https://www.forbes.com/sites/danielnewman/2018/07/31/five-iot-predictions-for-2019/#2ef2a7896edd>. [Accessed: 05-Dec-2018].
23. C. Qu, M. Tao, and R. Yuan, "A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes," 2018.
24. A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, *Blockchain and iot integration: A systematic survey*, vol. 18, no. 8, 2018.
25. A. J. GILL, J. A. STIRMAN, and C. E. GORDON, "Lactating adenoma of breast," *Tex. State J. Med.*, vol. 49, no. 4, pp. 231–233, 1953.

