

Application of Blockchain in Healthcare - A Systematic Review

Dr. Niharika P. Kumar
Computer Science and Engineering
B.N.M Institute of Technology
Bengaluru, India
niharika.kumar@gmail.com

Abstract—Blockchain has gained a lot of traction as a research area and has found application in a number of industries. The core aspects of blockchain i.e. security, privacy, confidentiality and decentralization make it an apt technology to use in the field of healthcare. Blockchain technology enables a decentralized and distributed environment with no need for a central authority. Transactions in a blockchain can be made secure and trustworthy by using cryptographic principles. In this systematic review, an analysis of state-of-the-art blockchain research in the field of healthcare is conducted. This paper provides a brief introduction to Blockchain. It discusses some of its applications and benefits in healthcare industry. The aim is to identify the potential applications of the blockchain technology and to highlight the challenges and possible directions of blockchain research in healthcare. The survey covers an overview of blockchain in healthcare, Electronics Health Records Management, Supply Chain management and application of blockchain in Healthcare and IoT

Keywords— *blockchain, healthcare, EHR, IoT, privacy*

I. INTRODUCTION

Blockchain, a digital ledger technology, was developed by Satoshi Nakamoto, and forms the basis for cryptocurrencies like Bitcoin, Litecoin, and Ethereum. Blockchain technology keeps track of transactions in a distributed ledger. Blockchain consists of a shared or distributed database used to maintain a growing list of transactions, called blocks. Blockchain technology, often called the chain of trust, can support transactional applications and streamline business processes by establishing the trust, accountability, and transparency.

Although blockchain was initially applied in financial industry, over the years, it has found application in many other industries including insurance, pharmacy, healthcare, legal contracts, travel industry etc. Applying blockchain in healthcare serves to improve patient care. It offers patients and caregivers the ability to share and store patient identity and healthcare information across platforms..A Blockchain consists of list of records called blocks. Each block in-turn comprises a set of transactions and is linked to its previous block forming a chain. A Blockchain is managed by a peer-to-peer network of nodes. This network validates new blocks using a consensus based algorithm. When medical research centers are provided with access to the healthcare data stored on Cloud based Platforms, it has a positive impact on medical research and innovation in the field of healthcare. That said, one should be aware of the sensitive nature of healthcare data and the hesitation of patients in sharing their data for research purposes despite the positive impact that such a sharing can have in providing optimal healthcare support to them. Patients fear about the implication of disclosure of their data and their identities which can have social, financial impacts and could potentially harm their employment and health insurance benefits.

This paper explores healthcare as a sector and enlists the application of blockchain in different aspects of healthcare. This paper is organized as follows: Section II describes, at a high level, the application of blockchain in the field of healthcare. Section III illustrates privacy issues related to EHR and the usage of blockchain to solve privacy issues. Section III delves on issues involved with sharing of EHR and the research undertaken to resolve the contentious issues related to sharing of EHR. Section IV deals with the supply chain management aspects related to healthcare and the different solutions for supply chain management. Section V explores the application of healthcare and IoT.

II. APPLICATION OF BLOCKCHAIN IN HEALTHCARE

In [1] authors review and analyze state-of-the-art blockchain research in the field of healthcare. The research work showcases the potential applications of Blockchain technology and to highlight the challenges and possible directions of blockchain research in healthcare. The paper proposes a further use of smart contracts and the introduction of less constraining consensus algorithms. The proposed system utilizes the distributed consensus protocol and validates the chronological order of generated transactions. This protocol provides proof-of-work, proof-of-stake, delegated-proof-of-stake, proof-of-importance, proof-of-activity, proof-of-burn and proof-of-deposit based blockchain validation.

In [2] various applications of blockchain in the field of healthcare are discussed. Some of them are: Medical data management where medical data is stored in the form of electronic health record by the use of blockchain. The paper also explores drug development where Blockchains can facilitate new drug development by making patient results more widely accessible. It can help reduce the counterfeit drug implications. The paper goes on to stress the benefits of blockchain technology in healthcare, data interoperability and security and how it could allow more systems to exchange and use information.

Mobile user controlled, blockchain-based system for personal health data sharing and collaboration is proposed in [3]. The system implementation has 3 parts: Personal Health Data Collection, Personal Health Data Integrity Protection and Validation-To facilitate scalable and efficient data processing and integrity protection. A tree-based method is developed to address aspects like integrity management of health data record, Data Sharing and Healthcare Collaboration. The paper proposes a system evaluation methodology, wherein, the system adopts a user-centric model for processing personal health data using blockchain network, thereby ensuring the data ownership of individuals, as well as data integrity.

The benefits of blockchain when compared to traditional way of storing healthcare records are analyzed in [4]. The

authors enlist various benefits of blockchain for healthcare, for example, Decentralized Management (Patient-managed health care records), Immutable Audit Trail (Unalterable patient records), Data Provenance (Source-verifiable medical records), Robustness/Availability (Reduced risk of patient recordkeeping) and Security/Privacy. The paper reiterates the fact that, blockchain is treated as a distributed ledger to store healthcare related data for sharing, exchanging, analyzing, recording, and validating purposes among stakeholders.

In [14] Authors present the different challenges in healthcare and the application of blockchain in order to solve these problems. The paper describes how cloud based systems store and manage electronic health records that pose security and privacy issues and the solutions to resolve these issues using blockchain. The paper also touches on the sensitive aspect of storing medical records in blockchain which might violate regulations. Hence the need to implement an off-chain storing of medical records and yet use the permanency aspect of block chain to maintain EHR. The author also alludes to a polynomial based block-chain structure and a Lagrange interpolation method to detect and remove fraudulent transaction in the blockchain. The paper also looks at protecting EHR via ECC cryptographic primitives.

A three layer, Ethereum and Interplanetary File System (IPFS) protocol based peer to peer network is proposed in [17]. The first layer, also called the user layer, consists of the users of the block chain network. The second layer is the block chain layer that implements the consensus based peer-to-peer network. The third layer that contains the system implementation of the smart contracts. Smart contracts includes the patient record rules as well as user access rules. Execution of these contracts was seen to take an execution time of anywhere between 18 seconds to 1 minute 48 seconds.

In [21] authors concentrate on the limitations of blockchain. Since the amount of data that can be added to a block is limited, the authors emphasize the importance of storing medical records offline. Public block-chain versus private block chain networks are explored as well.

A simulation based parallel healthcare system is proposed in [24]. The parallel healthcare system consists of artificial doctors, artificial patients and artificial hospitals. When a real patient is diagnosed and prescribed tests and intervention, the same data is fed to the parallel healthcare system. The parallel healthcare system runs simulations on the artificial patients and provides results which the real doctors can use to treat real patients. This parallel healthcare system was implemented and used to treat patients with Gout disease. The blockchain within this system consists of multiple clients like patients, doctors, hospitals etc. These clients generate the patients personal and medical data. Due to the size of the data, only the hash value of the patient record are stored in the blockchain. In order to achieve consensus among the nodes, delegated proof of stake method is used. The nodes in the consortium blockchain elect a certain number of trustees called delegates. These delegates collect the transactions in the blockchain network and then package them into a block. The responsibility of the other nodes is to verify the validity of the block and then appended it to the existing blockchain.

III. ELECTRONIC HEALTH RECORD (HER) MANAGEMENT

Privacy of Electronic health records is a very important aspect of healthcare. EHR contains sensitive information related to the patients, like their medical history, diagnosis etc.

The fundamental principle of using a block chain to store EHR and ensure privacy and consistency is proposed in [15]. A patients data is considered as a block and multiple blocks of health records of the same patient are maintained via links from one block to another. These blocks are distributed among multiple nodes of an infrastructure, and are not centrally stored. Each block contains a timestamp of its production, the hash of the previous block and the transaction data are stored in a block along with the EHR data. When new healthcare data for a particular patient is created, a new block is instantiated and distributed to all peers in the patient network. After a majority of the peers have approved the new block, the system will insert it into the chain. This creates a global view of the patient's medical history in an efficient, verifiable, and permanent way. If the agreement is not reached, then a fork in the chain is created and the block is defined as an orphan and is not added to the main chain. Once the block has been inserted into the chain, the data in any given block cannot be modified without modifying all subsequent blocks. In other words, modification can be easily detected. As block content is publicly accessible, healthcare data needs to be protected prior to the data being in the block. The main benefit of adding the EHR into a blockchain is the fact that agreement can be reached without the involvement of a trusted mediator and patients have control over their data ,medical history.

In [5] Authors propose a blockchain based framework called Ancile. Ancile, utilizes smart contracts in an Ethereum-based blockchain for heightened access control and obfuscation of data. The proposed system employs advanced cryptographic techniques for further security and has been designed to increase privacy and interoperability and focuses on the ownership rights of the patient. Ancile, uses six unique types of smart contracts for operation: Consensus, Classification, Service History, Ownership, Permissions, and Re-encryption.Using smart contracts. Ancile maintains cryptographic hashes of stored records and query links, confirming the integrity of EHR databases. The Ancile framework demonstrates a blockchain system that achieves a high-level of decentralization and at the same time give ownership and final control of EHRs to the patient.

In [8] authors propose a signcryption based blockchain system to ensure security of EHR. Patient's data is stored in database and the respective contracts are then added to the blockchain. Service provider generates related patient and provider relationship contract and then sends them as part of the transactions in the next block. This block will then be updated to the blockchain. Once a new block is mined and verified, the patient's patient-provider relation contract will then be added as a transaction into the newly mined block. The links to the new contracts will be added to the summary contracts. The service provider goes ahead and enforce the EHR changes in its database in parallel. By following this process, the EHR changes will get updated and then get recorded in the blockchain. The blocks uploaded to the block chain are encrypted. This ensures that the patient's data is secure. In future when there is a need to search patient's data, privacy preserving searches are initiated. Hence a smart contract based model is used along with an additional layer of signcryption and attribute based authentication. This ensures data authentication, data integrity (i.e. patients data is stored in a secure way and cannot be tampered), data confidentiality and yet achieve flexibility (i.e. patient can decide who gets to access the data), authentication as well as maintain an audit trail (of who accessed patient's data).

A cryptographically encrypted blockchain to store health records in blockchain is proposed in [16]. This proposed system employs public key cryptography to create and manage health identities. To ensure validity of the saved data, smart contracts are introduced into the system that maintain an immutable timestamped transaction log which includes information on the access granted to each user and information on what data is accessed by what user. The uniqueness of the proposal is to maintain the record in blockchain on the identity of the user accessing the health records. The proposed system has certain limitations though. This system may not be compatible with legacy systems. Once the EHR system migrates to blockchain based system, one cannot maintain interoperability with the legacy web-based client-server system. The other disadvantage of the system being that the clinical malpractice cannot be controlled as this design trusts the data being circulated is not being abused or misused.

Cryptographic solution is further extended for blockchain solution in [20]. Authors propose a solution that uses encryption to secure patient data and allows sharing of data for individual users as well as groups of users. Users are divided into different levels. Patient information is stored in the form of full data and summary data. Based on the level of the user, either the healthcare practitioner gets access to summary data of the patient or the complete user data. The encryption and access to user information is implemented at attribute level (and not at file level). Hence based on the type of user accessing the data, he/she may get only partial access to the patient file. In order to encrypt the data, authors use a combination of Elliptic Curve Diffie-Hellman Concatenation Key Derivation Function and the Advanced Encryption Standard Block cipher. The solution is implemented on Ethereum.

In [22], authors note that Health records can be segregated into two types. Health data that is generated in the hospitals (possibly signed by hospital and users also called EHR) and health data generated by the user (possibly using sensors. This is referred to as personal healthcare data, PHD). Authors propose to have two loosely coupled blockchains for these two types of data. EHR data has higher privacy requirement hence the data is stored off-chain. Only the verification of EHR data is supported on the block-chain. The block within this block chain shall contain five pieces of information, namely timestamp, medical-record hash value, hospital authentication information, patient signature, keywords and a brief description. The full copy of EMR shall be available with the hospital and the patient. A set of transactions are packed together to form a block within the block-chain. Authors propose 3 different ways of packing the data, namely, AP-Kth-Sum, Fair-first and TP&Fair.

IV. ELECTRONIC HEALTH RECORD SHARING

Most of the private health clinics and institutions usually use internal network to keep track of their patients but don't implement data sharing with other healthcare institutions, this may result in repeated tests and increase in expense of medical service as well as result in information islands about patients spread across multiple hospitals. Healthcare records face three main challenges: privacy (of patient details), security & Robustness (centralized records can become a central point of failure), and interoperability (of patient records across different hospitals). In [6] authors propose to use block chain and smart contracts to overcome the three challenges. A three layered architecture called BPDS is proposed. In the data

acquisition layer, doctors generate the patients records. Patient records are signed by doctors using CES scheme. Data storage layer stores these patient records and the indexes using cloud storage and consortium blockchain network. In the final layer the healthcare practitioners access these records (generated from data collected from different hospitals) to draw up health plans and evaluate the medical conditions. BPDS allows patients to manage their own EMRs. Sharing of EHR is sometimes necessary during emergencies. Doctors, nurses, health practitioners may need to access the EHR when a patient is in critical condition.

In [7] authors propose permission access rules using the smart contracts that determine access to EHR based on the emergency condition. The rules also determine the time duration for which there is a need to access the EHR of the patient. In addition, the paper proposes ways by which the patient can assign some limitations for controlling the permissions to EHR data. A permissioned block chain Hyperledger Composer technology network is used to store and access the patient records. This architecture consists of actors like the patient, doctor, emergency doctor and the database for storing (or updating) the EHR data. The patient's rules allow the EMT staff to access EMR data of the patient during emergency. Rest APIs are used for communication of the data. The ledger maintains the records of transactions that are added based on the consensus mechanism agreed between the participants.

Another research in [13] emphasizes on sharing of patient information that is mediated by the patients themselves. This involves multiple challenges like privacy, technology, security, the different incentives and governance issues that need to be addressed. The paper addresses these problems by introducing five mechanisms namely, digital access rules, data aggregation process, data liquidity, patient identity and data immutability. Digital access rules are the smart properties & rules that are assigned by the patient that determine how the patient records are shared. In the data aggregation process, patient is able to aggregate his health records spread across multiple entities by using blockchain. Data liquidity deals with the availability of data which is managed using immutable ledgers. The fourth aspect is the patient's identity. Each hospital currently maintains its own mechanism to identify a patient. Hence aggregating the patient information across healthcare centers is a challenge. Since blockchain uses public-key infrastructure, an individual's public key can act as the unique key to access and aggregate patient records across healthcare centers. The fifth pillar of patient data is data immutability. One should not be allowed to tamper patient's data. The "append-only" model of block chain fits perfectly with this requirement. Hence by employing blockchain patients data can be shared in a safe and secure way.

In [18] Authors propose a mechanism that ensures effective sharing of patient EHR and at the same time ensure privacy of the users. The system consists of a 3 layered network. The first layer involves the web or cloud platform that stores the patient information and records. These servers could either be the traditional servers or the cloud based servers. The second layer comprises of the cloud middleware that involves multiple virtual machines. This acts as a bridge between the first and third layer. The data is hashed in layer-1 before it is passed to layer-2 this ensures privacy of user data during the transition. The third layer comprises of the consortium blockchain network that manages the data sharing

and permissions management. The blockchain network involves three types of smart contracts. The first contract is called the Registry contract that maps each user to a smart contract called the patient data contract (PDC). The second contract which is the patient data contract contains the hash value of the patient medical record as well as the link to the medical record on the cloud. This ensures privacy and security as the hashed patient data is stored on the block chain whereas the actual data resides in the cloud. The third contract called the permissions contract, deals with sharing of patient data. The contract contains the unique key of the data requesting entity as well as patient's consent to share the data. This contract ensures that the data is shared only with the consenting entity.

V. SUPPLY CHAIN MANAGEMENT IN HEALTHCARE

Supply chain management is another area in healthcare where blockchain finds wide acceptance. Drug counterfeiting is a global problem that can introduce significant risks to consumers and the general public. If spurious drugs are introduced into the system it impacts the customers health and it also tarnishes the reputation of the original manufacturer on whose name the counterfeit is being sold.

In [10] A consensus algorithm is deployed within the supply chain network for medicines in order to mitigate the issue of transaction duplication (or double spending) by allowing nodes to verify true information. Once verified, information is then added to the hash value of a previous block, and the new sequence (ie, previous hash + newly verified information) is hashed to form a new block using a one-way hash function. The method used here is Pharmacosurveillance Blockchain System. The system prototype will be a distributed application (DApp) with a back-end distributed file system (DFS) supporting a private blockchain network. It will use smart contracts. The platform uses a consensus algorithm called Ethash. A second instance will be developed on the hyperledger fabric blockchain platform. The system implements 5 starting nodes, one for each participant in the traditional drug distribution model: the manufacturer, the wholesaler, the retailer, and the FDA, as well as an additional node that will house a consumer portal website. The DApp front end will be stored in all nodes. This interface includes a section that will display transactions performed along the distribution chains as well as detect anomalies and information discrepancies and display this information on a dashboard. It will trace the drug product as it moves along the chain and generate a timeline for each supply chain. Notifications will be displayed for shipments and anomalies detected in the chain. The application consists of Food and Drug Administration Account, Wholesaler and Retailer Accounts, Database consisting of the blockchain ledger, the smart contracts repository, the document repository and the drug distribution history along with radio-frequency identification tags, drug product pathway, anomaly detection and finally System Testing which evaluates benchmarks on various data corpus sizes and capacity of the system to reliably detect the anomalies.

In [11] the authors look at how blockchain helps to mitigate the supply chain issues as well as satisfy the Drug Supply Chain Security Act (DSCSA). DSCSA has stringent guidelines with respect to tracing and tracking of medication, serialization of products and processes, detection of suspicious and spurious products. DSCSA also lists down strict guidelines for wholesaler licensing. Block chain Projects

like MediLedger try to address these guidelines. Companies like iSolve are using Advanced Digital Ledger Technology to address the problem. Other companies like Walton use RFID and IoT along with blockchain to develop solutions to solve the supply chain issues for healthcare.

In [12] authors propose a blockchain mechanism to solve the supply chain issues via a three tier system comprising of blockchain, smart contract and multiagent system (MAS). The MAS, in-turn comprises of five layers, namely, producer layer that is responsible from the production, the processor layer called the processor agent, the transport layer comprising of transport agent, the retailer layer that has the retail agent and the blockchain layer comprising of the blockchain agent. Each layer generates a smart contract with the adjacent layer. For example the Transport provider agent creates a smart contract with Producer agent who in-turn creates a smart contract with processing agent and so on. Every transaction is then added to the blockchain thereby maintaining record of transactions. This helps in tracking all transactions.

VI. HEALTHCARE AND IOT

With the advent of Internet of things (IoT) based health monitoring devices, doctors can remotely keep a tab on the health status of patients. The IoT devices monitor and share the health data with the medical practitioners. Blockchain network can be developed for efficient management of such healthcare records generated by the IoT devices. In [19] authors proposes a five layered system comprising of an overlay network, cloud storage, health care providers, smart contracts implemented in a blockchain network and the patients equipped with healthcare IoT devices. The IoT devices that monitor patient's medical status shall upload the patient health status, onto the designated cloud storage. The authorized healthcare providers like doctors or insurance agents approved by the insurance companies have access to this data. The data is encrypted using both symmetric encryption technique (like SPECK) and asymmetric encryption technique. Digital signatures are used as additional authentication mechanism. In this system a smart contract is an agreement that get executed when a specific condition is met. For example if the blood pressure reaches a particular level then the information is stored in an encrypted fashion on the network and based on the smart contract, the relevant healthcare provider is alerted.

An IoT based healthcare system that uses private blockchain network is proposed in [23]. The sensors within the IoT devices shall measure the raw data. This data is sent to a master "smart device," say a smartphone or a tablet. This device formats the data and feeds it to a smart contract for full analysis along with customized threshold values. The smart contract evaluates the data and generates alerts to both the patient and healthcare provider, no confidential medical information will be stored on the blockchain or in the smart contracts. By not storing patient's confidential information the proposal ensures that HIPAA guidelines are complied. The system shall have an Ethereum solidity based private and consortium-led blockchain, that shall allow only the authorized viewers to read the blocks and a set of designated nodes to execute the smart contracts as well as verify new blocks.

VII. CONCLUSION

Over the past few years Blockchain has gained wider acceptance beyond cryptocurrencies into varying fields like

finance, healthcare etc. The need for security, integrity and confidentiality make blockchain a compelling case in the area of healthcare. Blockchain has been used in various aspects of healthcare like Electronic Health Records, Clinical Research, Medical Fraud Detection, Neuroscience Research, Pharmaceutical Industry and Research [2][25][26]. The research worked surveyed in this paper covers the different aspects of healthcare where blockchain has found wider acceptance. Future research is warranted in all these aspects of healthcare.

REFERENCES

- [1] M. Hölbl, M. Kompara, A. Kamisalic, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare" in *Symmetry*, vol. 10, no. 10, pp. 1 - 22, September 2018.
- [2] M. N. O. Sadiku, K. G. Eze and S. M. Musa, "Block chain Technology in Healthcare" in *International Journal of Advances in Scientific Research and Engineering*, Vol. 4, Iss. 5, pp. 154-159, May 2018.
- [3] X. Liang, J. Zhao, S. Shetty, J. Liu and Danyi Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications" in *IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, October 2017.
- [4] T. T. Kuo, H. E. Kim, and L. O. Machado, "Blockchain distributed ledger technologies for biomedical and health care applications" in *Journal of the American Medical Informatics Association*, vol. 24, iss. 6, pp. 1211–1220, September 2017.
- [5] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology" in *Sustainable Cities and Society*, pp. 283 – 297, February, 2018
- [6] J. Liu et al, "A Blockchain based privacy-preserving data sharing for for electronic medical records", *IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, November 2018.
- [7] A. R. Rajput, Q. LI, M. T. Ahvanooy and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain", in *IEEE Access*, vol. 7, pp. 84304-84317, May 2019.
- [8] H. Yang, B. Yang, "A Blockchain-based Approach to the Secure Sharing of Healthcare Data", In *Norwegian Information Security Conference*, pp. 1-12, November 2017.
- [9] J. Y. Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where Is Current Research on Blockchain Technology? — A Systematic Review", *PLoS ONE*, vol. 11, no. 10, pp 1 - 28, October, 2016.
- [10] P. Sylim, F. Liu, A. Marcelo, P. Fontelo, "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention" in *JMIR Res Protocols*, Vol. 7, Iss. 9, pp. 1-27, 2018.
- [11] K. A. Clauson, E. A. Breeden, C. Davidson, T. K. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An Exploration of Challenges and Opportunities in the Health Supply Chain", in *Blockchain in Healthcare Today*, pp. 1 – 12, March 2018.
- [12] R. C. Varaa, J. Prietoo, F. D. L. Prietaa, J. M. Corchado, "How blockchain improves the supply chain: case study alimentary supply chain", in *Procedia Comput. Sci.*, vol. 134, pp. 393 – 398, August 2018.
- [13] W. J. Gordon C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", in *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224–230, 2018.
- [14] J. B. Bernabe, J. L. Canovas, J. L. H. Ramos, R. T. Moreno, A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges", in *IEEE Access*, Volume 7, pp. 164908 -164940, October 2019.
- [15] 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?" in *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, January 2018.
- [16] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," in *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, July 2018.
- [17] A. Shahnaz, U. Qamari, and A. Khalid, "Using Blockchain for Electronic Health Records", in *IEEE Access*, Vol. 7, pp.147782-147795, September 2019.
- [18] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis and D. Tzovaras, "On the design of a Blockchain-based system to facilitate Healthcare Data Sharing" in *IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, pp. 1374-1379, 2018
- [19] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT", in *Sensors*, Vol.19, pp. 1-6, January 2019.
- [20] M. A. Cyran, "Blockchain as a Foundation for Sharing Healthcare Data", in *Blockchain in Healthcare Today*, pp 1- 6, 2018
- [21] C. Pirtle and J. Ehrenfeld, "Blockchain for Healthcare: The Next Generation of Medical Records" in *Journal of Medical Systems* Vol. 42, Iss. 172, pp. 1-3, July 2018.
- [22] S. Jiang et al., "BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange", in *IEEE International Conference on Smart Computing* pp. 49-56, April 2018.
- [23] K. N. Griggs et. al, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", in *Journal of Medical Systems*, vol. 42, Iss. 130, PP. 1-7, May 2018.
- [24] S. Wang et. al, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach" in *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942-950, Dec. 2018
- [25] A. A. Siyal et al. "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives" in *Cryptography*, Vol. 3, Iss. 3, pp. 1 - 16, Januray 2019
- [26] T. Kumar et al. "Blockchain Utilization in Healthcare: Key Requirements and Challenges" in *IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1-8, Nvember 2018