Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Decentralized Electronic Health Records Using Blockchain

Naresh Thoutam, Associate Professor, Dept. of Computer Engineering , Sandip Institute of Technology and Research Centre, Nashik, Savitribai Phule Pune University, Maharashtra,naresh1060@gmail.com
Thupakula Bhaskar, Associate Professor, Dept. of Computer Engineering, Sanjivani College of Engineering, Kopargaon, Savitribai Phule Pune University, Maharashtra, bhaskarcomp@sanjivani.org.in
Vuyyuru Krishna Reddy,Professor,Department of Computer Science and Engineering, Gandhi Institute of Technology and Management(Deemed to be University),Vishakhapatnam,AndhraPradesh. kvuyyuru@gitam.edu
A. Jayalakshmi, Professor and Head, Department of Computer Science and Engineering, PVPSIT-Prasad V. Potluri Siddhartha Institute of Technology, (Autonomous), Vijayawada, Andhra Pradesh. jvallabhaneni@hotmail.com

ABSTRACT: ***Research into blockchain technology has been fruitful for some time, and its advantages have been put to use in many fields. Security, protection, mystery, and decentralization are only a couple of the manners by which blockchain innovation could further develop the medical care industry. However, EHR systems have issues with storage, management, and the security of patient data. This study explains how blockchain technology works, how it might be applied to or affect the present SCM Registry systems, and the importance of having legal professionals on board. Government authorities currently considered trustworthy enough to handle transactions face serious threats from the proliferation of blockchains. The proposed method can automatically recover lost data and keep records of blockchain-based transaction management safe from outside interference. Data discrepancy during the transaction is also dealt with by the system. The primary goal was to specify the implications of blockchain technology on logistics and supply chains. The problems that are common in these areas were analysed, and the blockchain characteristics that are most important for addressing them were highlighted. We investigate the potential problems and gains of blockchain-based applications through a poll.***

INDEX TERMS: Blockchain, health records, electronic health records, decentralization, and scalability.

1. Introduction:

The introduction of an Electronic Health Record (EHR) involves transitioning from traditional paper-based record-keeping systems to digital platforms that store and oversee patient wellbeing data electronically. Electronic health records (EHRs) mean to expand the nature of patient treatment, the speed with which medical records are processed, and the accuracy with which they are recorded. Here's an overview of the key aspects involved in introducing an EHR system:

1.1 Understanding Electronic Health Records (EHRs):

Definition and Purpose:

Electronic health records (EHRs) are electronic variants of paper diagrams that incorporate data, for example, a patient's clinical history, conclusion, solutions, treatment plans, minimization dates, and sensitivities.

Benefits of EHRs:

EHRs offer several advantages, including improved patient care, enhanced communication and collaboration among healthcare providers, increased efficiency, reduced errors, better data security, and support for evidence-based decision-

making. radiology images, laboratory test results, and more.

Key Features Of HER:

- EHRs provide a centralized digital location for storing a patient's comprehensive health information.
- Electronic health records (EHRs) contain a plenty of data about a patient, including their clinical history, analyze, solutions, treatment plans, immunisation documents, allergies, test results, and vital signs, among other things.
- HRs allow healthcare providers to update patient records in real-time, ensuring that the most current and accurate information is always available.
- Maintained in a sharable digital format across multiple organizations.

Why we use blockchain technology

Using blockchain technology in Electronic Health Records (EHR) offers several compelling benefits and addresses critical challenges associated with healthcare data management. Here are the primary reasons why integrating blockchain into EHR systems can be advantageous :

- Enhanced Security and Data Integrity
- Consent Management and Privacy
- Immutability of Record
- Interpretability and Data Sharing

2. Literature Survey

Different kinds of IoT gadgets are included in the four-tiered basic IoT Blockchain fusion paradigm described in [1]. The model considers the utilization of a dispersed document framework for putting away monstrous measures of IoT information. Then, a Machine-to-Machine(M2M) independent exchanging framework is proposed on the Ethereum blockchain as a contextual investigation for a blockchain-based Web of Things application.

It is proposed in [2] that a blockchain-empowered edge-registering stage called Edgence (EDGe + knowledge, Figure 1) be utilized to proficiently deal with huge scope dApps in IoT situations.

According to [3], HCloud is an established JointCloud environment for serverless Internet of Things (IoT) applications. HCloud makes it possible to construct an IoT server with fewer servers by redistributing its tasks across many clouds in accordance with a predefined strategy.

As per [4], there ought to be a decentralized gasified help trade stage where arrangement suppliers can make and take demands for administrations in a completely independent, distributed way.
During the course of operations, costs and decisions to trade services are determined by gasification policies that are calibrated to meet organisational objectives.

IoT health devices for the elderly or those with special needs can be integrated into a gesture-based secure interaction system, as described in [5]. The system stores user IDs and health data from IoT devices in smart homes using a distributed blockchain consensus.

A seed generation technique and a public key management scheme based on blockchain technology are presented in [6]. To begin, should keys be generated using some kind of random seed generation scheme? Seeds are made using out-of-band correspondence and equipment variety to decrease the probability of a man-in-the-center assault and figuring out.

It has been established that there is a problem with security and privacy in IoT systems, as reviewed in

[7]. Second, Blockchain technology has some answers to the problem of safety. The analysis is broken down into its component parts, such as the enabling technology and the integration of IoT technologies.

One such mobility-related implementation experience is presented in [8] for the Smart Toll Transaction application. In this paper, we present an expected response by showing how simulated intelligence empowered Multi-Specialist Frameworks and ongoing brilliant agreements among Vehicles and Costs can use arranging, navigation, and conveyed learning capacities at the gadget level.
A content selection technique for edge cache nodes is described in [9]. This approach makes better use of cached data and decreases the time it takes to transmit data by using a Markov chain model. Slides of contents are stored in the secondary cache to increase the scope of cached content and decrease load times for the end user. As a means of increasing cache space and catering to users' preferences for localised material, the adoption of regional node cooperation has been made.

As stated in [10], To provide more options and less reliance on utility companies, this framework is based on the sharing economy and makes it possible for households to trade energy with one another. Concurrently, new possibilities for storing, transporting, and delivering renewable energy are made possible by the proliferation of electric vehicles and the growth of vehicle-to-grid (V2G) technology. Vehicle-to-Grid (V2G) technology could allow for more decentralised power generation and distribution.

In the context of local energy markets, our physical demonstrator shows how V2Genabled automobiles can be beneficial in terms of economic gain, total power balance, and consumed renewable energy rate.

3. Functional Requirements:

3.1 System Feature-1 :

Modules included in the system are:

1. Admin
2. Engage in Business
3. Validation of blocks and blockchain creation
4. Verification of the Consensus Algorithm and restoration of the Blockchain
5. The Production of Results

Methodology for Implementation

We build a distributed ledger for cross-border e-commerce and keep track of all international information in separate databases.

Each node will have a copy of the transactional block.

A genuine blockchain is created when the same block is replaced on all nodes.

• Any DDL, DML, or DCL conditional inquiry will make the framework recover information from all information hubs and afterward commit the exchange.

When validating data servers, if a blockchain is found to be faulty, the system will immediately restore the entire blockchain from a network consensus.

We'll recover from runtime server attacks using our own blockchain and fix the problem permanently.

For all servers, the system will validate each transaction automatically.

3.2 Second System Component:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Decentralisation: Decentralisation refers to the process by which authority responsibilities and control are distributed to the various subunits involved. The blockchain operates decentralised and without a central authority. Instead, each participant in the blockchain (a "miner") receives a copy of the transaction ledger and contributes to the chain by validating transactions and adding a new "block." The network is user-to-user, or peer-to-peer, and it operates in a decentralised manner.

Model(s) of consensus: Data stored on the blockchain is protected by the consensus model(s). In, it is said that blockchain forks, consensus failures, dominance issues, validating nodes, and the subpar performance of the blockchain network are all possible outcomes should the consensus mechanism fail.

Transparent: In order to reconcile transactions that occur at regular 10-minute intervals, the blockchain network does a self-audit once every ten minutes.

Free and available to the public: Users of a closed-source, decentralised app must have faith that their data is secure from any centralised entity. Users are less likely to adopt closed-source software.

4. System Design:

4.1 System Architecture:

IN fig.3.1.1 system Architecture there are four modules namely Admin, Patient/user, Hospital, and Insurance Company. there we use some algorithms like peer-to-peer, hash function and mining, validation, recover validation, etc.

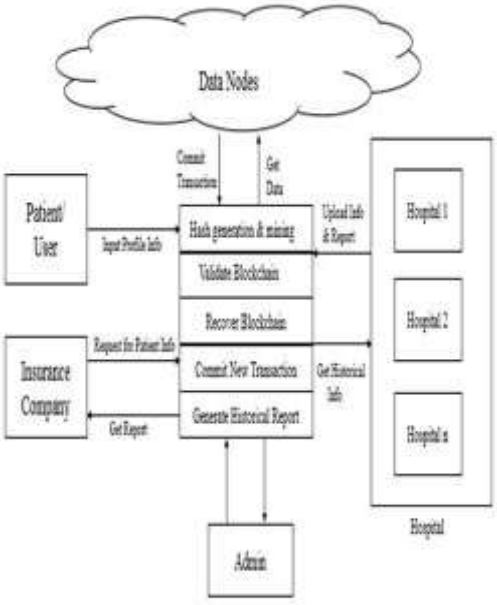


Figure 4.1: System Architecture

Process model

• Admin
• Make transaction
• Block Age and blockchain approval
• Agreement Calculation approval and blockchain recuperation
• Results Age
• The proposed technique is based on the central idea of using blockchain to store data about distribution in the supply chain.

The system generates reliable communication between several parties without the need for a mediator.

- The given string is used with a hashing algorithm to produce a hash value.
- Shared confirmation is utilized to check the exactness of the data before an exchange is completed.

• Assuming any chain is viewed as defiled, the ongoing server blockchain will be reestablished or refreshed.
• This will be checked until the inquiry is committed after all hubs have been approved.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

• Until a legitimate hash is made for an inquiry, it is really looked at utilizing a mining calculation.

4.2 Activity Diagram

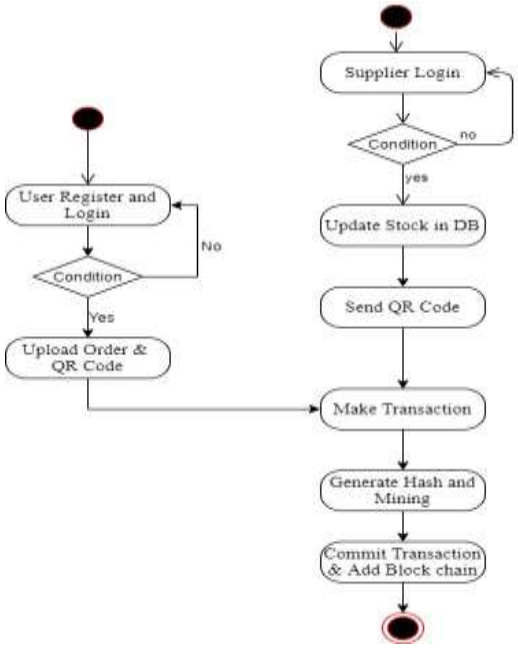


Figure 4.2: Activity Diagram

In the Activity diagram, we show all activities done by the Admin User and Distributor**.**

5. Algorithm Details:

5.1 Algorithm 1: Hash Generation

Input: data d,

Output: Created hash H from the input data.

Step 1: Type in your d

Step 2: Use the SHA-256 hashing algorithm.

Step 3: CurrentHash= SHA256 (d)

Step 4: Return CurrentHash

5.2 Algorithm 2: Protocol for Peer Validation

Input: Transactional User Inquiry, Blockchains for the Currently Active Node (CNode[chain]) and the Rest of the Nodes (Node-Chain[Nodeid] [chain])

Output: If the current query fails because of an invalid chain, recover and try again.

Step 1: The user creates a DDL, DML, or DCL transaction query.

Step 2: A current copy of the blockchain on the server

Chain ← *Cnode*[*Chain*]

Step 3: For each

$$NodesChain[Nodeid, Chain] \sum_{(i=1)}^{n} (GetChain$$

Stop for

To proceed to Step 4, insert I into NodeChain for each

To check for this, we'll use the condition: if (!.Equals NodeChain[i] with (Cchain))

Flag 1

Else, the Commit inquiry will continue.

Conditionally if (Flag == 1)

SimilarNodesBlockchian () = Count

Measure 6: Determine the Predominant Server

Node-specific invalid blockchain recovery.

7th Stage: Stop If

Stop for

3. Mining Algorithm for Producing Good Hashes

Input: Policy for Verifying Hash Values (P), hash-Value Now

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Output: Genuine hash

Step 1: The ITH transaction hash is computed by the system using Algorithm 1.

Secondly, if (hash-Val. valid with P[]), continue.

Genuine hash

Flag =1

Else

Flag=0

The Random Mine Once More

Third, if flag=1, only return a valid hash.

6. PRIMARY STEPS

In this part, we formally outline the prerequisites that make up the proposed framework. It explains the benefits of the software platform used to create this framework and how it was employed in its creation. The next section delves deeper into the framework's implementation, focusing on Ethereum and IPFS.

ETHEREUM

Using the same blockchain technology as Bitcoin, Ethereum is a decentralised digital currency exchange [13]. In 2015, Ethereum was initially announced with the goal of developing a decentralised, open-source, and programmable blockchain platform for smart contracts. The distributed systems administration that makes this innovation decentralized is something different that is shared. Ethers, the platform's native cryptocurrency, are also accepted here. The cryptocurrency can be transferred between Ethereum-based wallets. Ethereum also gives developers access to a language for modifying the blockchain, which was originally designed to facilitate the smart contracts that are Ethereum's primary selling point.

SHARING OF KNOWLEDGE

To engage with Ethereum from the outside world, one must perform a transaction. Users from outside the Ethereum network can use it to alter the data or records kept in the blockchain. The following components make up an Ethereum transaction:

The 20-byte from field identifies the message's originator.

• The recipient of the message, whose address is similarly 20 bytes long.

• Worth - the sum of money (wei) being sent to someone.

Message content is stored in the "Data" field, which is present if the sender so chooses.

Gas is the Ethereum blockchain's transaction cost, paid by the sender whenever a transaction is executed. The petrol cap and petrol price are included in each and every purchase.

The Gas Cost is the sum the purchaser will pay for gas as a feature of the arrangement.

GasLimit: the highest amount of petrol that could be charged for this exchange

INTELLIGENT CONTRACTS

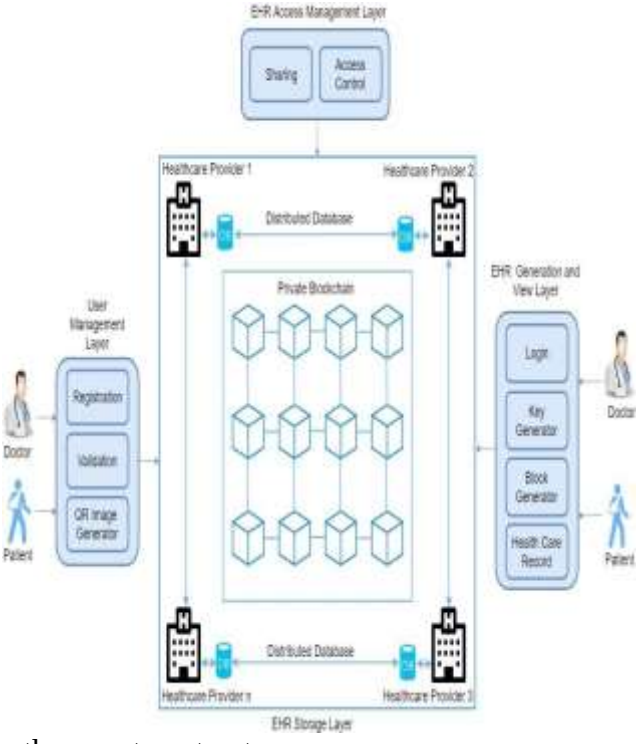
What we call "brilliant agreements" are pieces of code that might be utilized to do essentially any procedure on the blockchain. At the point when clients send exchanges, this code is done. They are protected against modifications because they run directly on the blockchain. Solidity is widely used in smart contract development, and it may be used to implement any conceivable action on the blockchain. EVM bytecode, which will be discussed in the following section, allows programmers to compile their code after writing the necessary operations. The resulting code might then be pushed to the Ethereum network for execution [13]. Ethereum's Solidity programming language is an enclosing environment for

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

JavaScript and Python code used in smart contracts.

EVM stands for ETHEREUM VIRTUAL MACHINE.

One of Ethereum's main selling points is its programmable blockchain. Users are given the option of developing Ethereum-based applications. DApps are what developers call the programmes they create on this system. They are a platform for decentralised applications (DApps) that contain many protocols in a single bundle. These DApps have "shrewd agreements" with client characterized "application code" to do a particular action. The Ethereum Virtual Machine (EVM) [12] is utilized to convey and run this code. Therefore, EVM is actually running the applications built with



the smart contract.

IPFS stands for "Interplanetary File System."

IPFS is a convention for putting away data in a decentralized way. IPFS ensures the integrity of data by prohibiting any modifications to files stored on the network. Any effort to modify IPFS-stored data would require altering the cryptographic identification used to access the data in the first place. A cryptographically generated hash value is embedded in every IPFS data file. It's a one-of-a-kind identifier for files on the Internet File Sharing System [12].

The IPFS convention is ideal for keeping urgent and hidden data because of its safe stockpiling strategy. The subsequent cryptographic hash may be saved money on the dispersed application, which would cut down on the number of compute operations performed via the blockchain.

The IPFS protocol relies on a P2P network that stores data and links in a structured data object called an IPFS object. The data is a random array of binary digits, and the association is an exhibit.

The IPFS protocol is implemented as described in [14]:

• Each IPFS-hosted file is given a distinct cryptographic hash

The IPFS network prohibits the presence of duplicate files.

• Content and index information for a node in a network are kept locally at the node.

7: The Suggested Model

The authorization blockchain and IPFS are two organizations that every one of the hubs on the organization (emergency clinics, patients, insurance agency, and so forth.) should be a piece of. However, not every node in the network is needed to store the complete blockchain permanently (so-called "light nodes").

Figure7.1: Proposed Model Diagram

In fig.7.1 Health Record Structure:

Patient Id
Gender
Age

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, October : 2023

Disease
Diagnosis
Location
Medication
Suggestion
Next Review
Notes
Date
Doctor's Name
Hospital Id.

Blocks and transactions in a Permissioned Blockchain are only validated by a predetermined set of users. In this execution of the blockchain, excavators don't need a motivator to mine blocks. In this way, in a consent blockchain, the idea of petroleum cost is pointless. The hospitals will play the role of miners in our simulation. Since clinics would have needed to pay cosmic totals to the associations taking care of their information and connection points without such a framework, they should have no trouble consenting to invest their processing power and mine blocks. Clearly Confirmation of Stake and Verification of Work can't be utilized as agreement calculations in the blockchain on the off chance that the thoughts of gas and ether don't have an impact in the framework. We along these lines propose Verification of Authority[15] as a suitable agreement approach for our utilization case. All transactions on a Permissioned Blockchain can never be altered, making it a permanent record of network activity. In this context, the word "activities" refers to things like:

In a hospital, a patient's information is documented.

• A patient viewing their medical history.
• A patient authorising or revoking the hospital's access to his or her medical records.
• A medical facility requests a patient's medical history;

Using the blockchain depicted in Fig6.1, the proposed system allows affiliated healthcare providers to securely store and distribute electronic health records. The proposed framework is separated into four particular layers relying upon their individual capabilities: the Client The executives Layer, the EHR Age and View Layer, the EHR Stockpiling Layer, and the EHR Access The board Layer.

Controlled Access Layer

The system's users are controlled via the User Management Layer. Those parts are the QR Image Generator Registration Module, the Registration Module, and the Validation Module.

The system has a registration module where users (doctors and patients) can enter their information. The user's information is gathered at the Registration section. The doctor is obligated to provide the patient's full name, cell phone number, email address, DOB, mailing address, and national identification number. All of the system's doctors are employees of one of the affiliated medical groups. Patients should give their full lawful names, government backed retirement numbers, birth dates, addresses, email locations, and health care coverage data. Likewise, both the specialist and the patient should enter a solid secret phrase.

Validation

The registered information of doctors and patients can be checked using the validation module. Doctors and patients who recently created accounts cannot use the healthcare system until their accounts have been verified and enabled. When a doctor registers with a

healthcare organisation, the organization's associated healthcare provider checks their credentials with the medical council to make sure they're legitimate. During the initial visit, a new patient's account will be activated. When a user activates their account, the system will produce a random 6-digit number and transmit it to their mobile device. The system uses the random number to validate the user's cellphone number and create a QR code.

Create a QR Code Image

After registering for the healthcare app, customers will receive a random number via text message that will serve as their login ID. The healthcare app requires the random number to be entered after the user has successfully logged in. The validation module ensures the user's entered random number is correct. After the authentication is complete, the QR image generator creates a QR code in base64 format using the user's username and hashed password. After that, the application's screen will show the QR image. The user can then use Google Authenticator or another similar software to scan the QR image. Other options include Authy, Clef, Authenticator Plus, Du, HDE OTP, etc. One-time passwords (OTPs) are generated from the scanned QR code. It's a prerequisite for using the healthcare app.

Generated Health Record Viewing Interface

The production of EHRs, accessing EHRs, and logging in all take place at this level. Login, Key Generator, Health Records, and Block Generator are some of the modules included.

Login

The healthcare system's users can gain access to the system with the help of the login module. It is protected by several layers of authentication. Users must enter their registered mobile phone number and the password they chose upon registration. When a user enters their mobile number and password, the system checks the information against its own database.

Medical History

After a visit to the specialist, an EHR is made that subtleties the patient's finding and any endorsed treatment. After the electronic health record has been generated, the patient is notified.

Produces a Roadblock

Patient consent is required for the electronic health record notification. Double-spending attacks can be prevented using patient EHR verification. When EHR confirmation is finished, the Block Generator module makes a block using the affirmed EHR information. The hash of the block's data is taken care of in the real block in a blockchain. The Key Generator Module's key is used to hash the electronic health record.

8. Final Thoughts and Future Directions:

The Final Thoughts

There are various possible roads for examination into the execution of Blockchain innovation in the exchange business, given the complexities of the field and the requirement for more steady and powerful data the executives systems. An interoperable design will without a doubt assume a critical part in different exchange use situations that stand up to practically identical information trade and correspondence challenges. Training of programmers and space specialists on the potential and constraints of this new innovation, and whether to construct a decentralized application utilizing a laid out Blockchain,

requires extra exploration on protected and effective programming rehearses for the utilization of Blockchain innovation in exchanges. The algorithm has determined the optimal balance between system complexity, efficiency, and ease of implementation. Empirical research has helped shed light on the rate at which new information is being added to the supply chain. However, there are still significant technological and data management barriers that prevent the blockchain from realising its full potential and being widely adopted for use in the healthcare industry.

8.2 Future work

To implement the proposed system on multiple peer-to-peer networks, with fog computing which reduces the transactional data processing time.

References:

References

[1] Gong, Xinglin, Erwu Liu, and Rui Wang. &Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading.& 2020 5th International Conference on Computer and Communication Systems (IC-CCS).IEEE,2021.doi:10.1109/ICCCBDA51879.2021

[3] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: "A Peer-to-Peer Electronic Cash System".Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem. J Gen PhilosSci 2008; doi:10.1007/s10838-008-9062-0.

[4] Kamel Boulos MN, Wilson JT, Clauson KA. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. Int J Health Geogr 2018;. doi:10.1186/s12942-018-0144-x.

[5] Holub A, O'Connor J. COINHOARDER: Tracking a Ukrainian improvement. Inf Sci (Ny) 2019; doi:10.1016/j.ins.2018.12.004.

[6] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., and Du, X., "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access,2017, doi.org/10.1109/ACCESS.2017.2730843.

[7]Xu, Jinliang, et al. &Edgence:" A blockchain-enabled edge-computing platform for intelligent IoT-based dApps.& China Communications" 17.4 (2020).

[8]Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways," Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control". J Med Syst 2016;40. doi:10.1007/s10916-016-0574-6.

[9]Koshechkin KA, Klimenko GS, Ryabkov IV, Kozhin PB. "Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation". Procedia Comput Sci 2018;126:1323 8.doi:10.1016/j.procs.2018.08.082.

[10] Comendador, B. E., Francisco, B. M., Medenilla, J. S., Nacion, S. M.,& Serac, T. B. (2015). Pharmabot: "A Pediatric Generic Medicine Consultant Chatbot", Journal of Automation and ControlEngineering, DOI:10.12720/joace.3.2.137-140.

[11]I. Grishchenko, M. Maffei, and C. Schneidewind, ''A semantic framework for the security analysis of Ethereum smart contracts,'' in Principles of Security and Trust. 2018, doi: 10.1109/OBD.2016.11

[12] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, ''HealthSense: A medical use case of Internet of Things and blockchain,'' in Proc. Int. Conf. Intell. Sustain. Syst. (ICISS), Dec. 2017,

[13] D. Vujičić, D. Jagodić, and S. Randić, ''Blockchain technology, bitcoin, and Ethereum: A brief overview," in Proc. 17th Int. Symp. INFOTECH-
JAHORINA (INFOTEH), Mar. 2018,

[14] interplanetary File System (IPFS). Accessed: Feb. 4, 2019. [Online]. Available: https://ipfs.io/.

[15] G. Jetley and H. Zhang, "Electronic health records in IS research: Quality issues, essential thresholds, and remedial actions," Decis. Support Syst., , Nov. 2019.

[16] K. Wisner, A. Lyndon, and C. A. Chesla, ‘‘The electronic health record’s impact on nurses’ cognitive work: An integrative review,’’ Int. J. Nursing Stud., Jun. 2019.

[17] M. Hochman, ‘‘Electronic health records: A ‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., Apr. 2018.

[18] Q. Gan and Q. Cao, ‘‘Adoption of electronic health record system: Multiple theoretical perspectives,’’ in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014,

[19] T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen,A. M. Aalto, and T. Heponiemi, ‘‘Experienced time pressure and stress: Electronic health records usability and information technology competence play a role,’’ BMC Med. Inform. Decis. Making, Aug. 2019.

[20] M. Reisman, ‘‘EHRs: The challenge of making electronic data usable and interoperable.,’’ PT, Sep. 2017.

[21] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, ‘‘Electronic health record breaches as social indicators,’’ Social Indicators Res., Jan. 2019.