I.J. Intelligent Systems and Applications, **2022, 5, 1-13**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2022.05.01

Blockchain Management and Federated Learning Adaptation on Healthcare Management System

Safiye Turgay
Department of Industrial Engineering, Sakarya University, Sakarya, Turkey
E-mail: safiyeturgay@yahoo.com, sencer@sakarya.edu.tr

Received: 13 April 2022; Revised: 11 June 2022; Accepted: 06 August 2022; Published: 8 October 2022

Abstract: Recently, health management systems have some troubles such as insufficient sharing of medical data, security problems of shared information, tampering and leaking of private data with data modeling probes and developing technology. Local learning is performed together with federated learning and differential entropy method to prevent the leakage of medical confidential information, so blockchain-based learning is preferred to completely eliminate the possibility of leakage while in global learning. Qualitative and quantitative analysis of information can be made with information entropy technology for the effective and maximum use of medical data in the local learning process. The blockchain is used the distributed network structure and inherent security features, at the same time information is treated as a whole, not as islands of data. All the way through this work, data sharing between medical systems can be encouraged, access records tampered with, and better support medical research and definitive medical treatment. The M/M/1 queue for the memory pool and M/M/C queue to combine integrated blockchains with a unified learning structure. With the proposed model, the number of transactions per block, mining of each block, learning time, index operations per second, number of memory pools, waiting time in the memory pool, number of unconfirmed transactions in the whole system, total number of transactions were examined.
Thanks to this study, the protection of the medical privacy information of the user during the service process and the autonomous management of the patient's own medical data will benefit the protection of privacy within the scope of medical data sharing. Motivated by this, proposed a blockchain and federated learning-based data management system able to develop in next studies.

Index Terms: Blockchain management, federated learning, healthcare management, differential entropy approach, machine learning.

1. Introduction

With the development of technology, health systems and information sharing are of great importance in terms of protecting personal information. The rapid growth and spread of computer and information technologies, the quick increase the data volume and the use of data in the right place and at the right time are of great importance. In particular, the need to protect electronic medical records has gained importance with the increasing amount of data. The use of these various features and accurate data during the diagnosis of patients provides convenience to both the patient and the physician and helps the patient to be treated accurately and quickly. In this context, the patient's data confidentiality and privacy are also important in terms of protecting personal rights. When a doctor diagnoses the disease, he/she tells the patient about past illnesses, physical needs, etc. It is common to ask questions about precise and accurate medical record files undoubtedly providing a more reliable reference for a doctor. The big medical data application is becoming more and more comprehensive and brings with it problems such as data privacy.

Maintaining the confidentiality of sensitive data in electronic medical records is a research hotspot. With the developing technology, the use of IoT and cloud computing technology for data storage cannot be as effective as the blockchain approach. In case of storing data with cloud computing or IoT techniques, patients may not be able to access information about where and how their data is used. At the same time, data manipulation with traditional data storage methods may occur. Such negative situations cause the personal information of patients to be accessed and changed. Medical data privacy also takes a success here. However, it prevents correct analysis due to changing information. When data is leaked or changed, it cannot be calculated accurately and the required results cannot be obtained. In addition, patient information, data confidentiality and access are also important. Algorithms need to be developed to prevent unnecessary sharing of medical data while improving privacy protection.

Access control is also an important part of data security. During data access control, the privacy control and security situation of the objects in the data becomes more difficult. In this article, Shannon's entropy is used in the process of measuring and evaluating information[1]. With the information entropy used in an integrated structure with

the blockchain, it is possible to reuse the information and store it in parts.

The proposed parallel-based queue simulation model provides fast performance which has been studied. M/M/1 queue model was used for memory pool and M/M/C queue model was used for federated learning. With the blockchain-based architecture, medical information was stored and data redundancy was prevented. With the simulation process, the parameters of delay, information retrieval, waiting time, queue time, processing time, output, usage and response time were examined.

The remainder of the article is organized as follows. Section 2 presents the theoretical background of the basic concepts; section 3 reviews existing blockchain and unified learning-based healthcare management systems. Then, section 4 briefly explains the research method. Section 5 discusses how proper blockchain based decentralized identity management can help ensure interoperability among the healthcare management system. Finally, section 6 discusses the results of the proposed method.

2. Related Study

With the developing technology, patient electronic medical records have increased, which are widely used in the e-health system, and are also used for successful patient treatment and patient follow-up. The blockchain and federated learning structure help to securely store and process harvest tracking information. Analyzed through various medical devices and sensing devices and recorded as signals, data or images are collected in the timely and safe delivery of health services to patients [2,3]. Some of the researchers are working on blockchain, unified learning, IoT and smart systems applications. Qi et al. used the blockchain federated learning structure to model the dynamic system for the traffic flow system [4]. On the other hand, Qu examined the medical chain role structure in detail together with the blockchain structure [5]. They analyzed different application patterns in the blockchain structure. Shi et al. evaluated the electronic health record system structure and applications together with the blockchain structure [6]. They examined the patient record structures in the database and examined the distribution structures and partial representation of the data in the block system. They looked together with big data, IoT, and edge computing. They also reviewed previous work on the development of blockchain architecture. On the other hand, Singh et al. examined the interaction forms of smart grid technology and cloud computing structure. They analyzed the quality of datasets and evaluated metrics (parameters) in performance analysis [7]. Alam et al. examined the developments in the blockchain architecture [8]. Ali et al. discussed the latest developments in the blockchain and federated learning architecture for IoT and their expected future developments and statuses [9]. According to Rahman et al. demonstrated in practice how the federated learning structure can be applied in health systems with the application of the Internet of Health Objects [10]. Di et al. reviewed Blockchain 3.0 applications [11]. Xiao et al. developed a model that improves the quality of the network structure by considering it in the form of query matrix, key matrix, and value matrix within the federated learning structure. They analyzed the performance of the model developed with the confusion matrix used [12]. Mojtab et al. examined the pharmaceutical blockchain structure and proposed a model [13]. Nguyen et al. examined the blockchain structure for the 5G network structure [14]. On the other hand, Saxena et al examined blockchain-based solution proposals for IoT security [15]. Lim and Rahmani have included the health management system structure along with the IoT load inference structure [16]. Uddin et al. It included the adoption process of blockchain implementation in IoT [17]. On the other hand, Singh et al. It included blockchain and artificial intelligence applications within a sustainable smart city structure[18]. Polap and colleagues discussed intelligent medical system structure with unified learning and blockchain technology[19]. Abdallah and Faizal reviewed the blockchain in fourth industrial revolution[20] . Anwar et al revieved the blockchain technology[21]. This work proposed and implemented entropy-based integrated unified learning in blockchain architecture.

3. Blockchain Based Federated Learning

Blockchain architecture consists of six layers: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. The data layer is the data storage layer, which is the weakest layer in terms of data security. Therefore, the fact that the confidentiality is random makes this layer more reliable. The network layer is the layer that provides communication within the blockchain structure[22,23]. At the same time, all network transmission is carried out through this layer, and private communication can integrate the confidentiality of information differently. This layer uses a consensus algorithm to ensure that untrusted parties in the consensus layer blockchain reach an agreement and meet in one spot. The incentive layer deals directly with the money/token data and it is essential to maintain data privacy in this layer. In this layer, information privacy provides the noise addition algorithm of differential privacy. In the contract layer, all functions and mechanisms in the proposed model are defined here by code. Ensuring data privacy with different smart filtering takes place in this layer. The last layer is the application layer where certain vulnerabilities and privacy threats like data analytics attacks can act similarly.

A client-server database (traditional database) represents a database located on a server in blockchain architecture. However, client applications are written to access the database. The database client uses an open database connection configured on the client side by the administrator Fig. 1. The client software then attempts to establish a secure connection. The system is high faults tolerant due to central database management. Due to its vulnerability to attacks,

this central system can be compromised.

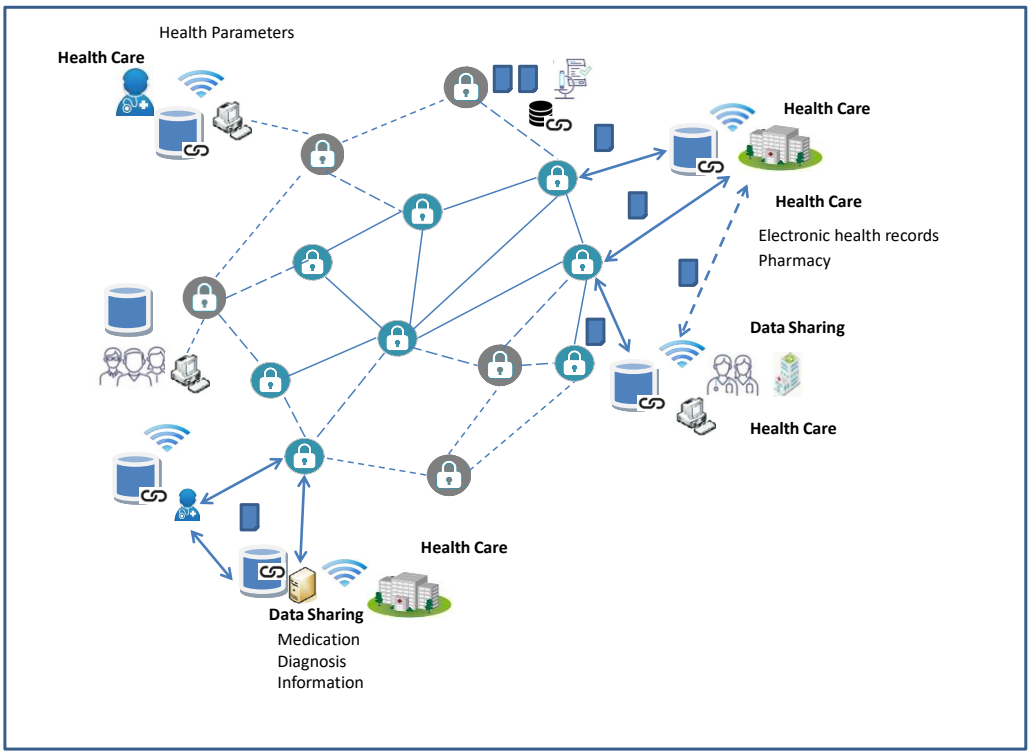

Fig.1. Data sharing model

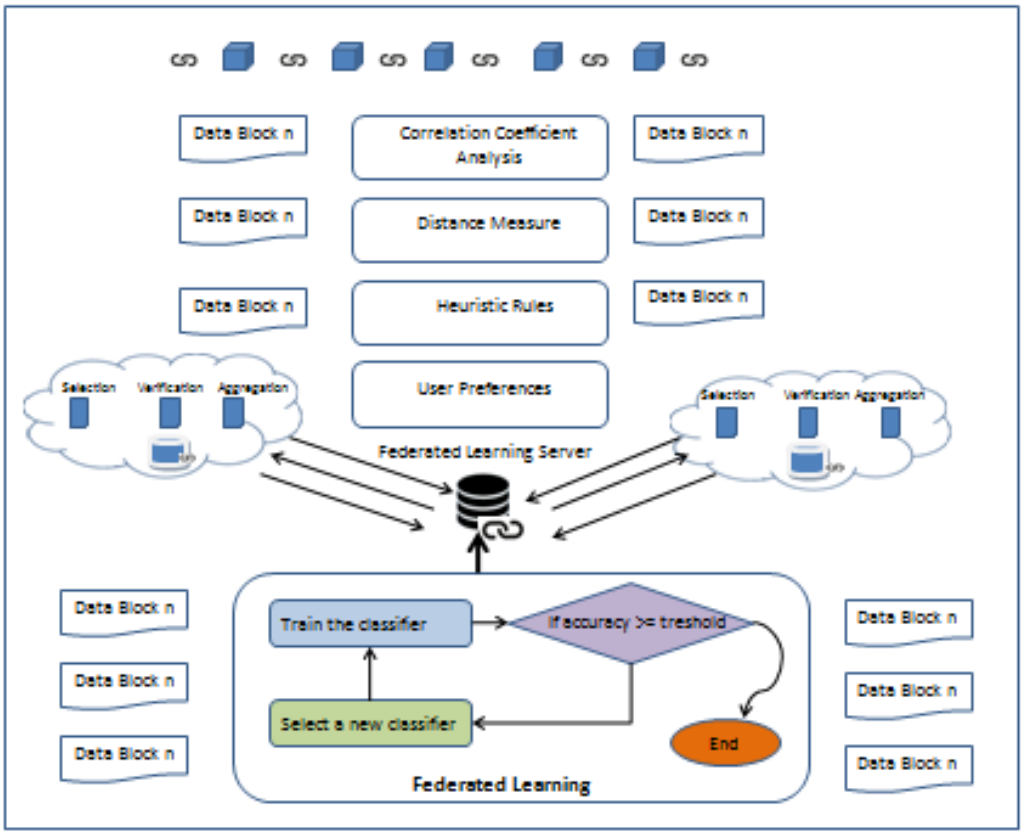

Fig.2. The blockchain-based federated learning model

Blockchain has a decentralized record structure, which can keep different data belonging to different organizations together, and this complex data structure also increases the security of the data. On the other hand, each node where the data resides can have different records and organizations and there is no need for trust between the nodes. Data can be easily protected due to the independent operation of the nodes in the system with blockchain technology,. Each

participating node can represent a different unit and belong to organizations, and units can operate independently without the need for trust between nodes. Federated Blockchain is a structure that allows participants to participate in the system in a certain hierarchy, and with its autonomy structure, it can allow the responsible user to respond to more than one situation at the same time. Only predefined members have the right to manage certain actions at different levels (in Fig.2).

A model proposal is made in this study to ensure the safety of medical data to increase security and responsiveness. In the blockchain network, information is securely stored thanks to private and public keys. The information is encrypted by the end user using the public key, while the private key decrypts the block of information received from the sender.

It is a privacy-preserving, distributed machine learning approach that trains data on a common platform instead of collecting local data for federal learning center model training. Participants' participant data may contain sensitive information and is stored in local storage, while other details are evaluated within the blockchain[24,25]. Initially, each user uses local storage. After the information is evaluated, the data is transferred to the global model and stored in an encrypted, distributed environment. The repeating information event ($T \in \{1,2,\ldots, T\}$) is represented by the time parameter. The federal learning process steps consist of three stages. These steps are listed below.

Step 1: In order for the process to begin, participants must register on the central server. The contact information and all the information of the users are located on the central server, and the level of importance in the system is determined by associating the participant with the wo variable and the t parameter.

Step 2: At this stage, the local education model is activated using local data with the permission of the participant. R here

$$\arg\min_{w\in R} F_k(w) = 1/G_k(x+a)^n = \sum_{i\in T_k} f_i(w) \tag{1}$$

The local model trained the account the participant loss function status. ω is the weight of the local model, and $f_i(\omega)$ represents a local loss function. While ω_{T+1} characterizes the regional model described by ω_T in the initial state after training. ω is the weights of the local model, and $f_i(\omega)$ represents a local loss function.

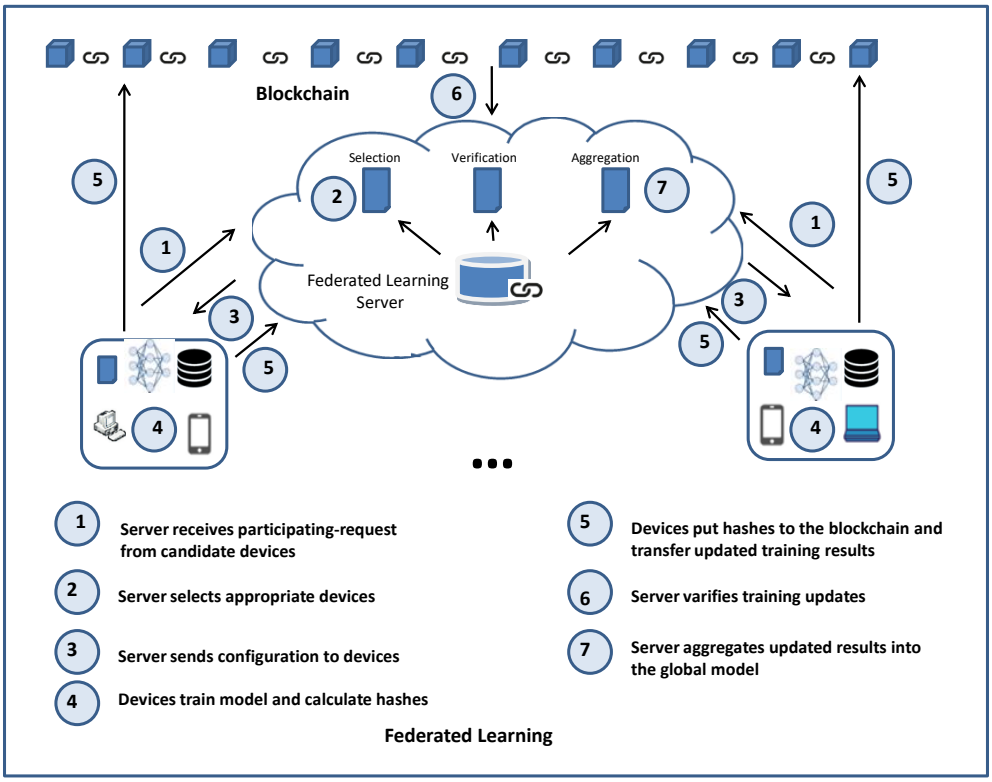

Fig.3. Blockchain-Based Participant Selection for Federated Learning [26]

Step 3: Local model update processes are also performed using the aggregation algorithm to update the global model with the participant.

$$F_k(w) = 1/G_k(x+a)^n = \sum_{i\in T_k} f_i(w) \tag{2}$$

$$w_{t+1} \leftarrow w_t - \frac{1}{K} \sum_{k=1}^{K} F_k(w) \tag{3}$$

Finally, the central server sends the new global model, creating a new block environment, including qualified local model updates, through consensus algorithms (ω_{t+1}).

- Local Model Training: For local model updates, each patient record is sent to the nearest miner with the differential entropy method in the local data set.
- Model Update Verification: The miner actually performs the machine learning process here, enabling us to reach the necessary correct data. Miners are employed to validate local model updates collected to obtain certain coin rewards. The miner also takes into account the process of obtaining useful information and rules from the data, taking into account the parameters that affect the quality of the data.

The process of storing and analyzing data is used in the gradually structure of the blockchain to prevent medical information leakage[27,28]. Federated learning, on the other hand, is used as a preliminary analysis process to determine the importance of data before moving to the blockchain stage. At this stage, the variability of the data was analyzed by the entropy method, considering the existing data and all other data, the importance of the data and its structure with all other data. The privacy level is set according to the legal authorization status of medical information users. The control of medical information leakage and security situations will be discussed in detail in the algorithms to be developed.

3.1. Algorithm

The algorithm structure considered the patient treatment outcome; using the drug status used the obtained outcome rules can be created according to the basic characteristics of the patient by comparing the local patient information with the treatment results at the same time in the study. Local learning in the federated learning process includes the following stages:

- **Stage 1:** Blockchain initiation: A smart contract is a set of instructions or criteria followed by nodes in the network to initiate data transmission from the other node. These conditions must be met in order for communication to be established. The smart contract is then deployed.

1- Model selection is performed.
2- Selects the relevant participants (ie local nodes) for the training situation.
3- Variables stored in local nodes are determined

```
BeginProcedure
Input:
    a)p:Objectofstructureinsmartcontractb)patient_idc)patient_named)patient_agee)patient_emailidf)patient_
    date :g)patient_gender
        BeginProcedure
        Step-I
                p.id=patient_id;
                p.name=patient_name;
                p.age=patient_age;
                p.email=patient_emailid;
                p.date=patient_date;
                p.gender=patient_gender;
        Step-II
                patient_list[patient_id]=p;
    EndProcedure
EndProcedure
```

4- Local training results sent by the participants are accumulated.

- **Stage 2:** Web3 Injection: After copying the ABI and applying the smart contract to our network, we get an ABI contract address. This address is used to transmit data to be sent over the blockchain with the smart contract. We use the regular web3.js API to communicate with our local network.
- **Stage 3:** Data Transmission: After successful network setup using Metamask,

5- An entropy-based model is created, including global aggregated results.

Data is routed through Algorithm - 1, the basic data entry algorithm is summarized in the smart contract. After successful completion, data is passed through the web3.js API and stored on the blockchain. Hospitals, service providers or patients can use Algorithm - 2 to retrieve data from the blockchain defined in a smart contract.

6- The updated model is shared with the participants again.

BeginProcedure
Input:
a)*p*:Objectofstructureinsmartcontractb)*patient_id*
BeginProcedure:
Step-I
patient_memoryp=[*patient_id*];
End Procedure
Output:
Returnalldatainsidetheblockchain
EndProcedure

7- Training ends when the updated model reaches the required threshold value.

– Patient identifiers can be used by organizations or blockchain
– Definitions entered by patients are processed by the smart contract. After the data is verified, the data is printed from the blockchain to the screen.

8- The proposed model also helps to establish the rules to be used in the decision support system within the system.
9- Encryption is used in the process of collecting and distributing data securely. With the structure proposed in this study, the block chain structure, which creates a safer and stronger firewall in the information storage process, was preferred.

After saving the data to IPFS it generates us a hash_id which we point with the associated id via Algorithm. Hospital providers or patients can get hash_id from the blockchain defined in a smart contract. From this hash, providers can retrieve and access data using IPFS.

– After Metamask's transaction verification, the data is sent to IPFS and hashed with the corresponding ID and transferred to the blockchain using the injected web3 API.
– Patient identifiers will be used by organizations or caregivers to search for them.
– The entered ID is then processed by the smart contract. After data validation from the hash recorded in the blockchain, the data is retrieved from IPFS and printed to the screen.

Requirement for the design process
The proposed model is capable of achieving the following results:

- The patient's privacy must be protected.

4. Performance Analysis

Performance analysis is handled together with the structure in which local learning and global learning processes are evaluated. In this context, high system performance also indicates high data security. The most basic component in ensuring information security in the blockchain structure is that the information is stored in parts, not as a whole. The information is divided into parts in a certain order, and the incidence of intervening and infiltrating the system by accessing the information at that time is very low. The data is stored in the system in blocks and combined in a certain order in the source file creation and made ready for reuse. It is very difficult to access these files in part or in their consolidated version. It is very difficult to reach the patient data in this proposed model and to make any changes on it.

During information security, the patient's password information will also ensure that the information is displayed as a whole.

The criteria taken into account in the blockchain performance analysis are;

- Transaction latency
- Transfer speed
- Transaction data size
- Scalability
- Fault Tolerance

The files are stored in the asymmetrically encrypted blockchain and can be decrypted with the private key. Without the patient's private key, the data cannot be accessed and therefore cannot be decrypted. The attacker must have the password to access the file. Here, an asymmetric structure and the need for a private key show that the file has a high reliability.

In the blockchain structure, data theft is very difficult in the process of protecting files with smart contracts. Accessing the files with the hash algorithm included in the smart contract and at the same time replacing the real file with the fake file is like impossible. Medical record data can only be accessed by persons with higher authority, as well as the patient and doctor with the private key, with the access control protocol and private key used with privacy protection,

With the following theorem and proof, it can be seen that data can be stored piecemeal with the differential entropy approach and machine learning algorithms can be applied to these data at the same time.

Theorem: Let q(x) be any density satisfying $\int q(x)\chi_i\chi_j dx = \sum_{ij}$ .Let

$$p = \mathrm{N}\left(0, \sum\ \right) \tag{4}$$

Then $h(q) \le h(p)$.

Proof: We have

$$0 \le \mathrm{KI}\left(q \| p\right) = \int q(x) \log \frac{q(x)}{p(x)} dx \tag{5}$$

$$= -h(q) - \int q(x) \log p(x) dx = -h(q) - \int p(x) \log p(x) dx \tag{6}$$

$$= -h(q) + h(p) \tag{7}$$

$$\int q(x) \log \frac{q(x)}{p(x)} dx \tag{8}$$

However, to achieve long-term sustainability in healthcare, three key challenges need to be addressed: data security, data privacy, and social acceptance of the deep learning process.

5. Analysis

Storing, archiving and securing patient information falls within the scope of strict data protection regulations. Both the use of this data with machine learning algorithms in order to make the right decisions by analyzing and obtaining the rules that can help in the diagnosis of the disease, as well as ensuring the security of the data, also presents us with contradictions. Within this scope, the data should be analyzed correctly and its security should be provided simultaneously. With the proposed federated learning blockchain algorithm, this process is aimed to be realized. With the proposed model structure, it is possible to train the data and determine the rule structure by using the ML algorithm over a large number of medical data sets without combining the e-health data.

This study consists of two parts. Local learning and global learning are the collection of information in the local learning center federated learning system and performing the pre-learning process, and then the information is included in the blockchain in fragmented blocks. The local training results are taken and sent to the blockchain, where the data is stored in fragmented blocks and combined in case of need for the information again, making it ready for use. Here, there are active and passive education and learning processes. By applying the differential entropy method within the central federated learning structure, the data is prepared in the global storage structure (Fig.4.).

Step 1: Incoming information for local education is pre-assessed and sent to the relevant blockchain for global education.

Step 2. Local Computing: This server runs local learning algorithms, updates the information results from global learning, provides information to the general learning algorithm and controls the incoming information, in fact, it acts as a bridge between existing patient data and new data.

Step 3. Collection of Local Models: It covers the process of collecting the data obtained as a result of global learning and processing these data in federated learning, which is also local learning. Data privacy, security, and comprehensive key encryption features are also used during the process.

Step 4. Global Model Update Step:3. Taking into account the data structures and data obtained in the step, the update process is performed with global learning. The information obtained after the update process is shared with the

stakeholders.

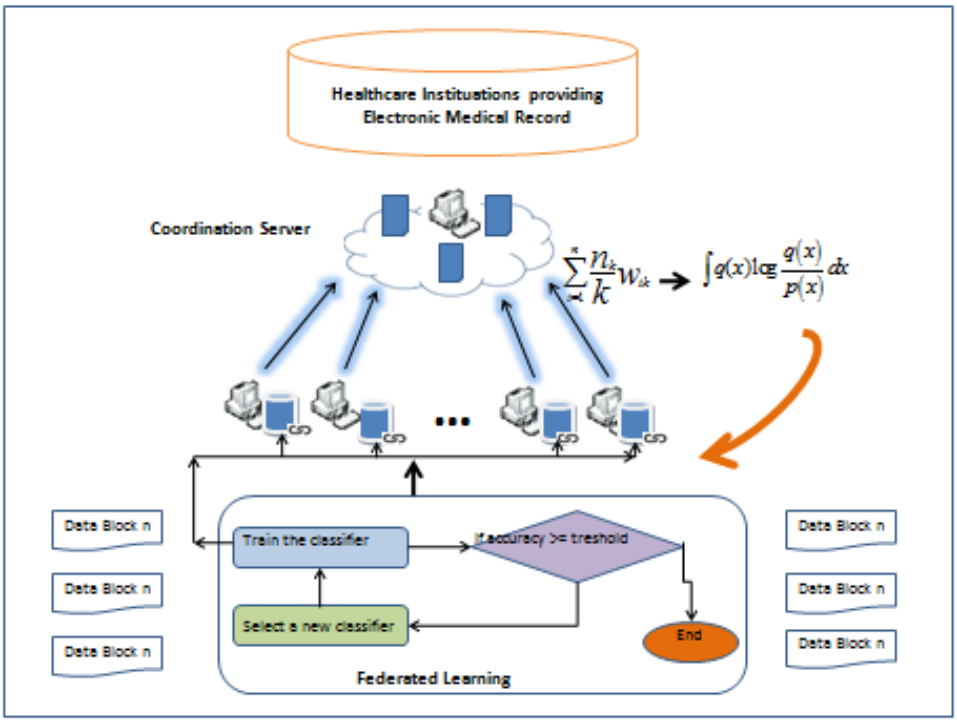

Fig.4. Workflow cycle in a central FL framework consisting of four steps.

The cycle is repeated until the required accuracy threshold is achieved until the global model reaches sufficient accuracy in the global learning process as mentioned above. In short, the result of local learning and the result of global learning should completely overlap.

The stand-alone operation of centralized databases weakens system security and may pose problems in maintaining the confidentiality of patient data. In this context, a hybrid model has been proposed and the federated learning system has been discussed together with the blockchain structure. At the same time, with the differential entropy used, it will be possible to evaluate the information with criteria such as the area covered, the content of the information, and the degree of importance.

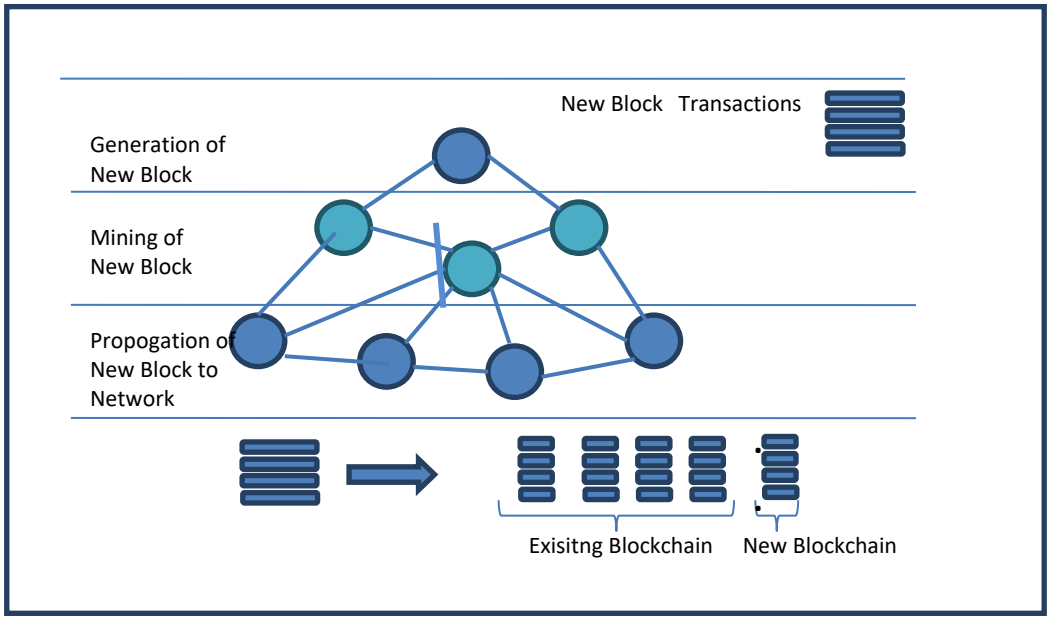

Fig.5. Transactions in Blockchain Network.

An entire blockchain, especially mining only transactions, in a single row; block generation process and queued transactions are assumed for transactions [29]. (In this paper, simulation modeling of a blockchain system using queuing theory is proposed. The proposed model includes memory, blockchain pool, and mining process. The M/M/1

structure provides a simplified simulation to model mining in the memory pool. It uses the M/M/c queue in the repository, the proposed model is based on entropy-based computation on key index structures such as the number of transactions per block. Mining time of each block, number of transactions per second, number of memory pools, waiting time memory pool, number of unconfirmed transactions in the whole system, the total number of transactions, and number of blocks created (Fig.5) [30].

Adding a new bn block requires verification of its true relationship to the previous block. After the block b_{n-1} is verified, it is added to the chain. New blocks are created at a frequency every 10 minutes [31]. A temporary placeholder or shared space used by all users with the memory pool used in the system. The memory pool has a structure that grows or shrinks according to the size of the information coming to the instant system.

$$B = [b_1, b_2, b_3, \ldots, b_{n-1}, b_n] \tag{9}$$

Mining time, on the other hand, aims to find the right target with billions of iterations. With the correct data discovery of the blocks, that is, the discovery of the nonce, the new block is added to the local blockchain. The process works in two directions, it is the recognition of the new currency and the determination of the rewards event and making the choice that will increase the system performance. The actual number of blocks and the average time created every day in cryptocurrencies reveal the dynamic structure of the new mining power, that is, the system.

$$Hash = (BlockHeader \cup nonce) \leq D \tag{10}$$

$$B_n = \frac{T}{B_t} \tag{11}$$

To maintain the time interval between blocks mined by miners, there is a difficulty level [32].

$$\text{Target}_{new} = \text{Target}_{old} \frac{t}{2028 \times 600}$$

where t is the total time spent mining for the previous 2028 blocks. Fig.6 shows the suggested model framework and Fig.7 represents the simulation model's printout.

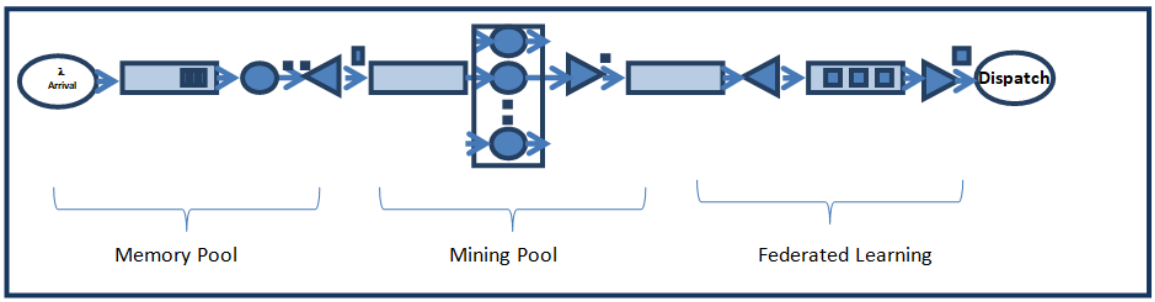

Fig.6. Suggested modelling framework for simulation

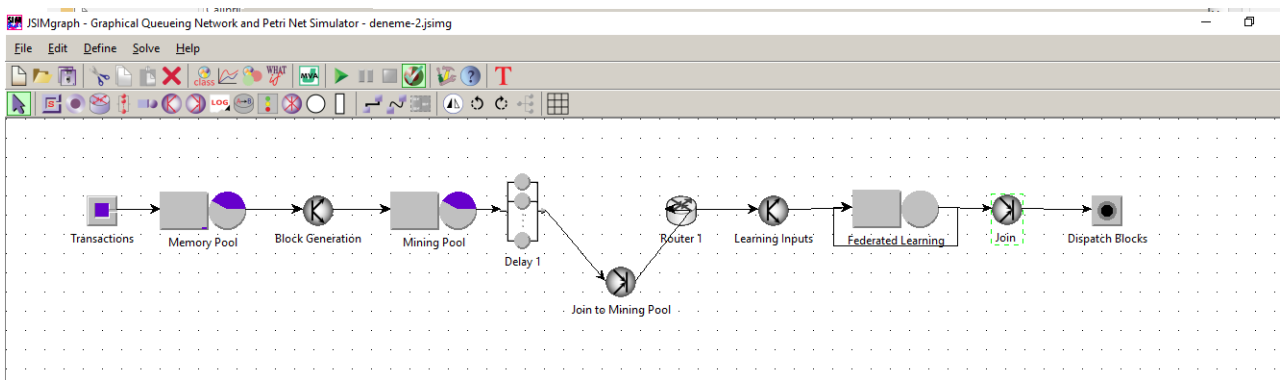

Fig.7. Simulation Model for Blockchain Management and Federated Learning using JSImgraph((JMT, Politecnico di Milano, 1.0.3, Milano, İtaly)

A mining pool with a single queue and multiple servers or miners with a single server as a memory pool is typically slightly larger than the size of a block. However, a true blockchain network consists of hundreds of millions of

users and miners. Mining pool with memory pool one M/M/1 and one M/M/c queue is configured using Federated Learning with M/M/1 queue. Figure 5 and 6 show the proposed system model of the blockchain. Table 1 shows the results.

Table 1. Suggested simulation framework results

Source		Policy	FCFS
Transaction Arrival Rate	5.48 (λ(s))	Queue Capacity	98
		Drop Rule	BAS
Memory Pool			
Transaction Dispatched from Mempool	0.1572 (λ(s))	Federated Learning Queue	
Policy	FCFS	Mining Rate	0.04567 to 0.07089 (1/μ(s))
Queue Capacity	∞	Number of Miners	50
Fork		Policy	FCFS
Number of Jobs	98	Queue Capacity	70
Number of Tasks (Block)	1	Drop Rule	BAS
Policy	FCFS	Execution Parameters	
Finite Capacity	98	Number of Total Transactions	532438
Drop Rule	BAS	Initial Mempool Transactions	64684
		Initial Transactions in Fork	98
Mining Pool Queue		Simulation Time	86400s
Mining Rate	0.07243 to 0.07089 (1/μ(s))	Repetition Seeds (days)	60
Number of Miners	100		

Toggles are used to update the blockchain when the smart contract is triggered. A transition is created for each smart contract using enumerated JavaScript. The Truffle framework automatically calls the transition or numbered JavaScript file. A certain amount of coins is spent from the account used for each pass. When the user registers, the metamask prompts the user for confirmation. After the user is authenticated, the transactions are added to the pending transactions pool. Next, a variable contract with certain parameters (ABI, contract address and price) is created using the web3.eth.contract method; where ABI is the variable that stores the contract interface and another variable stores the address of the deployed contract in the blockchain. network. The price is determined by the number of coins used in each transaction. The function then reads the data from the web page and stores it in the variable of the contract. If any contract parameters do not match the data block, the data transfer is not started and an error message is printed in the console log. Fig. 7 shows the memory pool simulation results and Fig. 8 indicates the customer numbers.

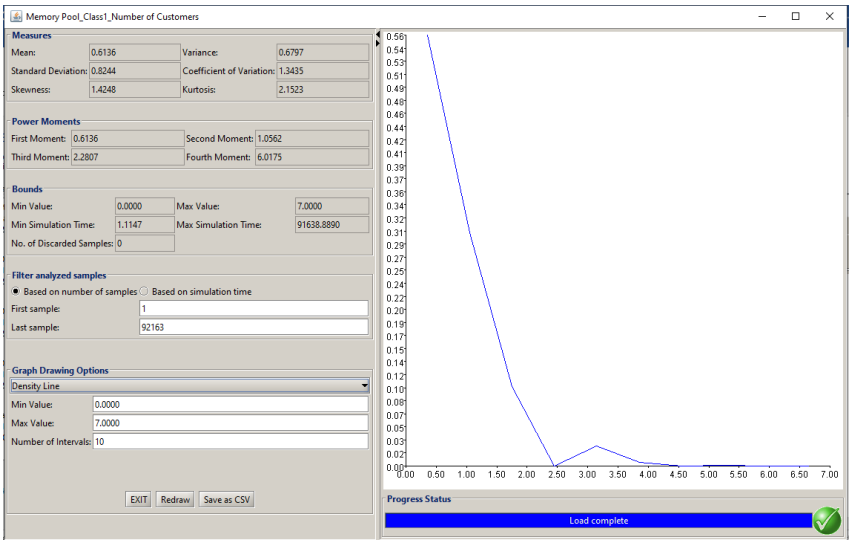

Fig.8. Memory pool simulation results

6. Conclusion

A high degree of accuracy in the learning structure indicates high performance, however, data security and privacy will need to be considered. Fast processing of patient records is possible with the effective use of local and global learning. Here, local learning is possible with federated learning and global learning is possible with blockchain structure.

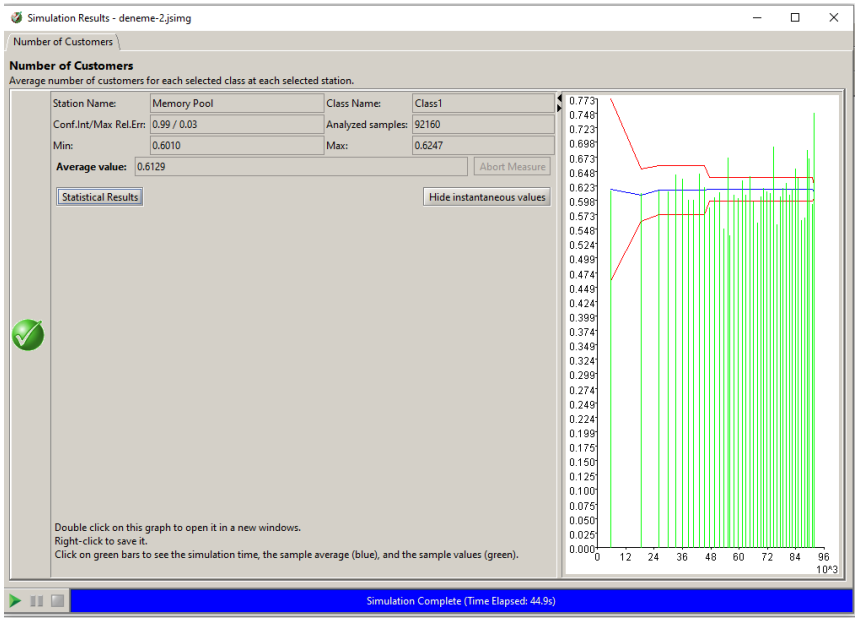

Fig.9. Suggested simulation model's customer numbers

The proposed blockchain-based architecture reduces data redundancy and overcomes security challenges for storing and retrieving medical information in IoMT applications. The simulation process is carried out by considering a queue-based model in the application. The proposed model was used to represent the blockchain application with paralleled systems. The model was examined with two main groups, cryptocurrencies and the structure of patient information control over the internet were discussed. Estimation of mining units, rewards received, optimization, estimation of mining capacity, system performance and strength can be tested using the proposed model.

Due to the decentralized nature of the blockchain, a secure system is used where the third party does not edit the data. Anyone who requests access is notified by the owner. It also supports multi-user authentication, allowing users to allow third-party access for data interoperability, which is crucial in the healthcare industry. Next generation applications over the Internet can be simulated by taking into account the parameters of latency, information retrieval, waiting time, queue time, processing time, output, usage and response time.

The simulation model was tested by considering the queue model of the theoretically modeled blockchain. The M/M/1 queue for the proposed modeled memory pool, and the M/M/C queue for combining integrated blockchains with a federated learning structure are preferred. With the proposed model, the number of transactions per block, mining of each block, learning time, index operations per second, number of memory pools, waiting time in the memory pool, number of unconfirmed transactions in the whole system, total number of transactions, and rules generated from the information in the blocks were taken into account. The model structure was simulated by only modelling the classical blockchain structure and then comparing the model structure by considering the federated learning structure.

As a result, effective use of data security, data privacy, and differential entropy learning process is required to improve the quality of data management in healthcare The proposed model includes: 1) the confidentiality of the training dataset, 2) the collection of global model gradients through a private Blockchain-mediated organization, 3) the process of securing federated patient information with local and global learning by blockchain and off-chain, 4) data set sharing, model training, and encrypted sharing status between federated customers; and 5) a model structure integrated with the differential entropy approach and reasoning processes is presented. An effective data management model is proposed with a confidentiality agreement and secure encryption structure with blockchain technology.

References

[1] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J., vol. 27, pp. 379-423, 623-656, July-Oct. 1948.
[2] F. Jamil, M.A.Iqbal, R.Amin, D.Kim, , Adaptive Thermal-Aware Routing Protocol forWireless Body Area Network. Electronics 8, 2019, 1–28.
[3] R. Kashyap, Applications ofWireless Sensor Networks in Healthcare, in: IoT andWSN Applications for Modern Agricultural Advancements: Emerging Research and Opportunities, IGI Global, 2020, pp. 8–40.
[4] Y. Qi, M. S. Hossain, J. Nie, X. Li Privacy-preserving blockchain-based federated learning for traffic, flow prediction, Future Generation Computer Systems 117, 2021, 328–337
[5] J. Qu, Blockchain in medical informatics, Journal of Industrial Information Integration, https://doi.org/10.1016/j.jii.2021.100258
[6] S. Shi, D. He, L. Li, N. Kumar, M. Khurram Khan, K. R. Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, Computers & Security 97 (2020) 101966.
[7] P. Singh, M. Masud, M. S. Hossain, A. Kaur, Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid, Computers and Electrical Engineering 93 (2021) 107209

[8] S. Alam, M. Shuaib, W. Z. Khan, S. Garg, G. Kaddoum,M. S. Hossain, Y. B. Zikria, Blockchain-based Initiatives: Current state and challenges, Computer Networks 198 (2021) 108395
[9] M. Ali, H. Karimipour, M. Tariq, Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges, computers & security 108 (2021)102355
[10] M. A. Rahman, M. S. Hossain, A. J. Showail, N.A. Alrajeh, M. F. Alhamid, A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city, Sustainable Cities and Society 72 (2021) 103083
[11] D. Di, F. Maesa , P. Mori, Blockchain 3.0 applications survey, Journal of Parallel and Distributed Computing 138 (2020) 99–11
[12] Z. Xiao, X. Xu, H. Xing,F. Song, X. Wang, B. Zhao, A federated learning system with enhanced feature extraction for human activity recognition, Knowledge-Based Systems 229 (2021) 107338
[13] S. Mojtab, H. Bamakan, S. G. Moghaddam, S.D. Manshadi, Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends, Journal of Cleaner Production 302 (2021) 127021
[14] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Blockchain for 5G and beyond networks: A state of the art survey Review, Journal of Network and Computer Applications 166 (2020) 102693
[15] S. Saxena, B. Bhushan, M. A. Ahad, Blockchain based solutions to secure IoT: Background, integration trends and a way forward, Journal of Network and Computer Applications 181 (2021) 103050
[16] R. Lim, R Madeira, Portugal Toward Semantic IoT Load Inference Attention Management for Facilitating Healthcare and Public Health Collaboration: A Survey, The 10th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2020) November 2-5, 2020, Procedia Computer Science 177 (2020) 371–378
[17] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, Blockchain: Research and Applications, PII: S2096-7209(21)00001-4, DOI: https://doi.org/10.1016/j.bcra.2021.100006
[18] S. Singh, P. K. Sharm, B. Yoon, M. Shojafar, G. H. Cho, I.H. Ra, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustainable Cities and Society 63 (2020) 102364
[19] D. Połap, G. Srivastava, K. Yu, Agent architecture of an intelligent medical system based on federated learning and blockchain technology, Journal of Information Security and Applications 58 (2021) 102748
[20] R.S. Abdullah, M.A., Faizal, Block Chain: Cryptographic Method in Fourth Industrial Revolution, I. J. Computer Network and Information Security, 2018, 11, 9-17
[21] S. Anwar, S. Anayat, S. Butt, S. Butt, M. Saad, Generation Analysis of Blockchain Technology: Bitcoin and Ethereum, I.J. Information Engineering and Electronic Business, 2020, 4, 30-39, ess.org/) DOI: 10.5815/ijcnis.2018.11.02
[22] N. Truong, K. Sun, S. Wang, F. Guitton, Y.K. Guo. "Privacy preservation in federated learning: An insightful survey from the GDPR perspective", Computers & Security, 2021, Nguyen Truong et al.: Preprint submitted to Elsevier
[23] Y. Lu, Xiaohong Huang, Yan Zhang, Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT, IEEE Transactions on Industrial Informatics DOI:10.1109/TII.2019.2942190, International Conference on Blockchain and Trustworthy Systems BlockSys 2020: Blockchain and Trustworthy Systems pp 112-125
[24] Y. Zhao, M. Cui, L. Zheng, R. Zhang, L.Meng, D. Gao, Y.Zhang. "Research on electronic medical record access control based on blockchain", International Journal of Distributed Sensor Networks, November 18, 2019
[25] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R.Mukkamala, M. Avital."Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation", Blockchain: Research and Applications, 26 May 2021, 100014
[26] K.Zhang, H Huang, S.Guo, X. Zhou, (2020). Blockchain-Based Participant Selection for Federated Learning. In: Zheng, Z., Dai, HN., Fu, X., Chen, B. (eds) Blockchain and Trustworthy Systems. BlockSys 2020. Communications in Computer and Information Science, vol 1267. Springer, Singapore. https://doi.org/10.1007/978-981-15-9213-3_9
[27] Y. Xinyi, Z. Yi and Y. He, "Technical Characteristics and Model of Blockchain," *2018 10th International Conference on Communication Software and Networks (ICCSN)*, 2018, pp. 562-566, doi: 10.1109/ICCSN.2018.8488289.
[28] S.Chen, X.Cai, X.Wang, Blockchain applications in PLM towards smart manufacturing. Int J Adv Manuf Technol (2021). https://doi.org/10.1007/s00170-021-07802-z
[29] Q.L.Li, J.-Y.Ma, Y.-X. Chang, Blockchain Queueing Theory, 2018. Available online: https://arxiv.org/abs/ 1808.01795 (accessed on 20 January 2019).
[30] RA Memon, J.P. Li, J.Ahmed, Simulation Model for Blockchain Systems Using Queuing Theory. *Electronics*. 2019; 8(2):234. https://doi.org/10.3390/electronics8020234
[31] N.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin. pdf (accessed on 20 January 2019)
[32] B.Biais, C.Bisiere, M.Bouvard, C.Casamatta, The Blockchain Folk Theorem, 2018. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3108601

Authors' Profiles

Safiye Turgay received her undergraduate degree from Istanbul Technical University, department of Industrial Engineering, master's and doctorate degrees from Sakarya University's department of Industrial Engineering from the Institute of Natural and Applied Sciences. She worked as a lecturer Bolu Abant ˙Izzet Baysal University Computer Programming, Computer and Teaching Technologies and Education, Business Administration, Sakarya University Management Information Systems. She is currently Associate Professor in the Sakarya University, Faculty of Engineering, Department of Industrial Engineering. She has many publications on multi-agent systems, fuzzy logic, decision support systems, production systems, multi-criteria decision making techniques and rough sets.

How to cite this paper: Safiye Turgay, "Blockchain Management and Federated Learning Adaptation on Healthcare Management System", International Journal of Intelligent Systems and Applications(IJISA), Vol.14, No.5, pp.1-13, 2022. DOI:10.5815/ijisa.2022.05.01