Lightweight Blockchain Framework For Medical Record Data Integrity

Viddi Mardiansyah[1] and Riri Fitri Sari[1*]

[1] Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok 16424, Indonesia
[*] Corresponding author. E-mail: riri@ui.ac.id

Received: Nov. 28, 2021; Accepted: Feb.21, 2022

Medical data record from the patient is private data that is very confidential and secure. Securing medical data records using blockchain can prevent unauthorized parties from seeing or changing the data. However, it has a drawback in creating a block known as a mining process that takes a long time and uses enormous resources. We proposed a lightweight blockchain framework for medical record data integrity in using resources that reduce the computational. Based on the work, to build a lightweight blockchain application, the Python programming language is used. The Flask micro web server is applied in illustrating the blockchain data, while the MIT App Inventor creates an Android application to read data from IoT devices. The IoT Implementation of this work has successfully been tested to retrieve data and store it in a blockchain framework. The lightweight blockchain discussed in this paper is a mining technique using leading-zero as a difficulty level factor while ensuring data integrity and security when creating a block. We compared the block-time generation required to make a block on this system with the block-time generation on the existing network such as Bitcoin, Ethereum, Dogelite, and Litecoin. From the difficulty level of one to five, the experiment results, the block-time obtained from 0.0012677 seconds to 34.5919193 seconds. Overall for a low level of difficulty has a faster duration than the existing network. Only at the fifth difficulty level appears to have a longer processing time than Ethereum, but still quicker.

Keywords: Lightweight Blockchain, Internet of Things, Sleep Apnea, Medical Record, Leading-Zeroes

http://dx.doi.org/10.6180/jase.202301_26(1).0010

1. Introduction

Blockchain can be implemented and used in the healthcare industry to ensure privacy. At the same time, it also provides a new way to protect the personal medical record data from the patient that can only be seen by themselves, the family, the doctor, or other related [1].

Garratt Hasenstab [2] stated that blockchain improves our live-in healthcare, social impact, and business travel. Blockchain has the potential to change the industry, not only for FinTech (Financial Technology). Some researchers are also trying to use blockchain in medical implementation [3–5], in the Internet of Things (IoT) [6–8], using cloud-based [9], and the other implementation of blockchains such as for transportation [10, 11], for economics [12, 13], for software engineering [14–16] , and power plants [17].

Blockchain technology described how to establish a set of decentralized trading systems without government interference [18]. Blockchain has the opportunity to transform the healthcare industry by securely maintaining and distributing patient data. Clinicians should ensure that the patient data is up-to-date. Lightweight blockchain is a system that offers lighter execution, encourages point-to-point IoT-Fog(Edge)-Cloud integration and autonomous platform interfaces to IoT applications for computation execution and communication [19].

Medical record data integrity means that data should be complete, accurate, consistent, and up-to-date. One of the essential questions in research is how to secure medical data from being stolen or modified [20]. Data integrity is not only used to guarantee the validity of data but can also

be used to verify data.

This paper proposes a new personal medical records system using a lightweight blockchain and the Proof-of-Work (PoW) concept as a consensus algorithm. Finding the leading zeroes is used as a mathematical target in the PoW concept. Cryptographic hash processing is implemented to ensure integrity and security while capturing and storing data from the patient using IoT devices. Because IoT devices have limited computational capabilities, in this paper, we will show difficulty in finding the most suitable leading zeroes to be used as targets in the PoW concept.

We summarize the contributions of this work as follows:

- We propose a lightweight blockchain architecture for personal medical record data management using the Proof-of-Work concept that incurs low computation and communication overheads compared to the traditional Bitcoin and Ethereum network. We achieve this by using the suitable leading zeroes as targets in the hashing process when creating a block in the blockchain network.
- We propose a solution for safer medical record data storage using blockchain technology. The process of securing the medical record data starts when received raw data from the IoT device and is sent to the server using a smartphone device. Then the medical record data will be wrapped into a block in the blockchain network.
- We evaluate the performance of our proposed lightweight blockchain and compare it with the Bitcoin network. Our experimental results demonstrate that our proposed design outperforms the Bitcoin and Ethereum network of block-time generation to process medical record updates.

This paper presented the work on lightweight blockchain for securing medical record data from patients with Sleep Apnea disorders. In Section 2, the concept of lightweight blockchain and medical data records is reviewed. Section 3 will be focused on the proposed system design and its implementation. In Section 4, the discussion on the results and discussion of the system using python-based and Flask micro-web is conducted. The final section is the conclusions of the work.

2. Review of lightweight blockchain and medical data record

2.1. Traditional Medical Data Record

Medical record data has an essential role in knowing the history of the illness and the patient's medical actions. The use of medical record data is vital for treating patients who have a history of persistent disease. To determine what medical treatments have been given and what medical treatments are suitable for treating the disease.

Currently, medical record data is generally stored using a client-server architecture with desktop or web-based modes in each hospital or health care provider [21–23]. Architectural design with this model will be handy when patients always visit the same hospital or health provider during their sickness because medical record data is appropriately stored in their systems. The problem will come up when the patient has to be referred to another medical treatment or another hospital. The patient has to start their medical data record from the beginning. This makes it difficult for health care professionals to make an appropriate prognosis or diagnosis of disease when necessary and makes it difficult for patients to have a broader view of their medical history.

In recent years, researchers and the industry have proposed many systems to solve this problem using cloud-based solutions [24, 25]. In a cloud-based system, medical record data is stored in the cloud so that hospitals or health care providers can access patient data more accurately. The weakness of using client-server or cloud-based data storage for medical records is using a centralized database system, making it vulnerable to access security disturbances by unauthorized people.

2.2. Blockchain

Blockchain technology is known to be reliable for securing data. Satoshi Nakamoto established the blockchain framework in 2008 by exhibiting an answer for a decentralized trust mechanism among obscure elements [18]. Bitcoin is the first implementation of cryptocurrency using blockchain technology to facilitate peer-to-peer payments that affected budgetary establishments. It uses cryptographical functions to conduct financial transactions and presents many cryptographic forms of money into the marketplace in the continued years. All cryptocurrencies are blockchains, but all blockchains are not cryptocurrencies. Most cryptocurrencies use blockchain technology to record transactions through a decentralized system. Another example of blockchain technology in the financial industry is Financial Technology (FinTech), developed in 2014. Blockchain in FinTech appeared for the first time as the distributed ledger of Bitcoin but has recently attracted consideration from practitioners and researchers [26].

Blockchain technology guarantees data integrity by establishing a secure encryption algorithm such as SHA-1, SHA-2, and SHA-256. This hashing crypto method creates

a solid and adequate hashing code from fixed-size data to strings of character. Blockchain uses SHA-256 that outputs 256 bits, and no two input strings can produce the same 64-character hash. This algorithm efficiently verifies data, file, and message integrity during the transaction, data identification, and event password verification [27].

Blockchain technologies can change existing business models and positively impact industries, governments, and societies [28]. Engineers who plan to build IoT always pay attention to the limited storage capacity and extensive data processing. On the other hand, the engineers who will implement the blockchain understand the blockchain structure and feasibility to process data and secure data even though it requires enormous resources.

The consensus algorithm is one of the most vital parts of building a blockchain network. One of the common and frequently used consensus algorithms is to use the PoW method. This consensus is used by Bitcoin [29] and Ethereum in their implementation. One of the weaknesses of this consensus is the use of energy that is quite large because miners will compete to solve a given puzzle to get rewards. As a result, the miner who fails to complete the puzzle will be in vain for his work. Currently, many ways have been done to overcome the problem of energy waste in this consensus.

2.3. Lightweight Blockchain

Lightweight Blockchain is a framework that offers a lighter performance than existing blockchain technology while applying authentication and encryption techniques to secure operations on sensitive data. The lightweight blockchain framework proposed by Tuli et al. [19] can facilitate end-to-end integrated relationships between the IoT and the fog (edge), and the cloud. This framework also supports the use of multi-platform software systems that are easily used. Fig. 1 shows the lightweight blockchain framework. In Fig. 1 scheme, the IoT device is a data-producing device or data collector. The equipment has a sensor to recognize the external environment state and an actuator that changes the command or executes it.

The Fog Gateway Network in Fig. 1 is used to bridge the IoT devices and distributed computing infrastructure. The Fog Gateway Network also helps the IoT devices be configured with an integrated environment to run the applications needed. The Fog Computational Nodes in Fig. 1 are devices equipped with core processors for processing, memory, storage, and bandwidth to perform lightweight blockchain operations. Processors are used to complete the computational process of leading-zero searches based on a predetermined level of difficulty. The difficulty level proposed in this lightweight blockchain does not change the data security but only affects the mining process duration for a node block.

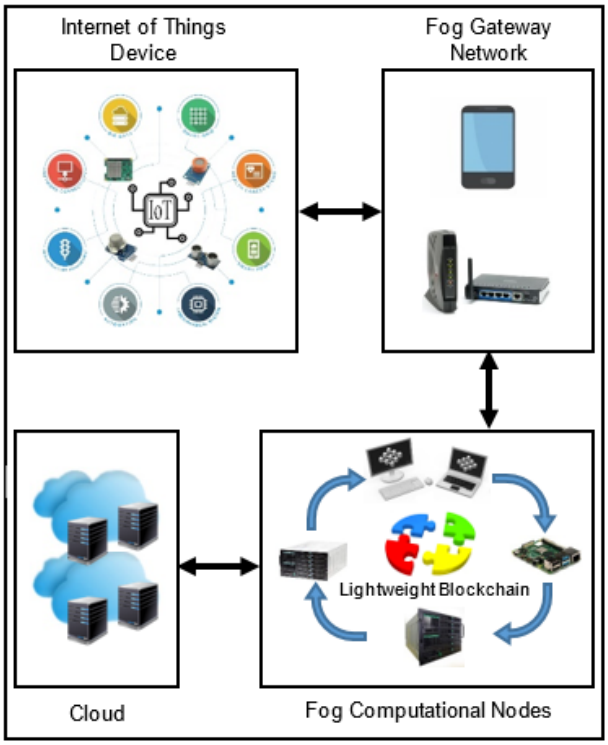

Fig. 1. Lightweight Blockchain Framework Scheme

The higher the value of the difficulty level defined, the longer the period creates a node block. The cloud in Fig. 1 can be used to run the IoT applications in a back-end if service requirements are tolerant of latency. With a cloud computing platform for the IoT, applications are accessible worldwide.

2.4. Leading-Zero(es)

Generating a blockchain network block using the PoW concept will succeed if it can solve a given mathematical problem. The mathematical puzzle used is to find the leading-zero(es) sequence in a word from the hash function using leading-zero(es) counting.

Leading-zero(es) counting is the procedure to count the number of consecutive zeroes that appear before the first nonzero number at the beginning of a word [30]. For example, the leading-zero(es) counting unit assumes n-bits data given to the counter is:

$$Lzc = Lzc_{n-1}Lzc_{n-2}Lzc_{n-3}\ldots Lzc_0 \quad (1)$$

The Lzc_{n-1} is the most significant bit (MSB) and produces the $\log_2 n$ bits of the leading-zero(es) count. For exam-

ple, if the data is 00111010, we will receive the leading-zero count of two because two consecutive zeros are found.

The mining procedure in blockchain consists of finding a hash that matches the target called the difficulty. The leading zeroes use as a target puzzle. The difficulty level is determined by the number of zeros found in the resulting hash output sequence.

2.5. Finding Nonce

A nonce is an abbreviation for "number only used once," which is a number added to a string of data transactions before it hashed. Nonce starts at zero and increases to countless numbers to find a hash value lower than or matches the target. The nonce controls all mining processes. The process of finding nonce is defined as follows:

$$\text{SHA256}\ (Tx + \text{nonce}\ ) = \text{LeadingZero}\ (\ \text{target}\ ) \quad (2)$$

Where Tx is the data transactions and "+" is the string concatenate operator. The target is the number of leading zeros.

2.6. Medical Record for Sleep Apnea using Oximeter

Sleep apnea is a disease that commonly attacks patients with cardiovascular disease. This respiratory disorder is one of the critical mediators of cardiovascular disease. This respiratory disorder generally occurs when the patient is asleep. We can notice respiratory problems from the length of time the patient stops breathing during their sleep. As a result, their organs, especially the brain, may not get enough oxygen intake and low sleep quality. This kind of symptom can come with tiredness, which can cause death [31].

Hypopnea patients can experience no inspiration for low airflow while generally can last for 10 seconds or more. This symptom is related to decreased arterial oxyhemoglobin saturation and or can stimulate electroencephalographic (EEG). These oxygen interruptions can cause a wide variety of symptoms linked to some airflow conditions [32].

Apnea patients can stop breathing as many as 40 times per minute. They are awakening, feeling as though they had little or no sleep, which is true as they have been fighting for oxygen all night [33]. Apnea and hypopnea can be classified as very severe diseases due to reduced oxygen intake to the brain, causing various complications [34].

Apnea-Hypopnea Index (AHI) measures sleep apnea severity. The AHI is the average number of apneas (pauses in breathing) plus the number of hypopneas (periods of shallow breathing) that occur per hour. At least 10 seconds duration is needed to collect the events for the Index of apneas and hypopneas. Table 1 is the category of Apnea-Hypopnea Index (AHI) measures, according to the American Academy of Sleep Medicine (AASM).

Table 1. Apnea-Hypopnea Index (AHI) Category.

Apnea-Hypopnea Index (AHI)	Rating
Less than 5	Normal
5 until 15	Mild
15 until 30	Moderate
More than 30	Severe

The calculation of AHI is by dividing the number of events by the number of hours of sleep [32–35]. The data processing is processed based on Eq. (3).

$$AHI = \frac{(A_n + H_n)}{n} \quad (3)$$

AHI is the Apnea-Hypopnea Index, An is the number of apneas (pauses in breathing), Hn is the number of hypopneas (periods of shallow breathing) that occur, and n is the duration in hours.

Oxygen saturation is an essential element in the understanding of patient care. Oxygen is tightly regulated within the body because a lack of oxygen can lead to many acute adverse effects on individual organ systems [36, 37]. Oxygen saturation measures how much haemoglobin is currently bound to oxygen compared to how much haemoglobin remains unbound. Pulse oximetry is a non-invasive and painless test that measures blood oxygen saturation level (SpO2). It also can detect the heartbeat rate in beats per minute (BPM) and show them in its LED. The oxygen level for ordinary people is usually between 90% to 100%. It should be cautious if the oxygen level is below 85%. Sleep apnea patients can use the pulse oximeter on the tip of their fingers. This tool will immediately take measurements [38].

This Oximeter uses haemoglobin nature, which can absorb light and natural pulses of the bloodstream in the arterial tract to measure the body oxygen levels. Its equipped with a light source, light correction, and microprocessor to compare and calculate the difference between oxygen-rich and oxygen-deficient haemoglobin. One side of this tool contains red light and infrared. Both types of light are transmitted through the body tissues to detect the light found on the other side of the device. More abundant in oxygen, haemoglobin absorbs more infrared light, while those without oxygen absorb red light [39]. Another pulse oximeter is already built-in on the Android smartphone device, but it uses only single light to detect blood oxygen saturation.

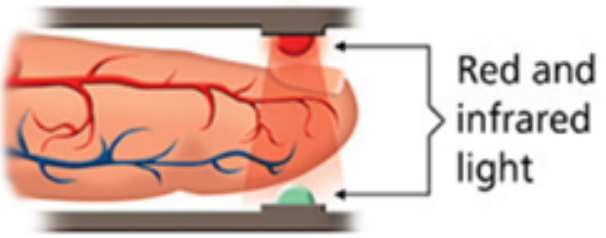

Fig. 2. The Oximeter Sensor Method of Works

The illustration in Fig. 2 shows how the oximeter sensor works.

In this system, the smartphone is used as a connecting gateway with the IoT device. A Bluetooth oximeter has IoT functions to capture data received and sent to a smartphone for further processing. We built an application using MIT App Inventor software for Android smartphones [40]to ensure that data accepted can be processed.

MIT App Inventor is an intuitive, blocks-based visual environment that allows everyone, even children, to build fully functional apps for Android devices. An MIT App Inventor project consists of components and program blocks that provide these components [41].

2.7. Data Integrity in Medical Record

The definition of data integrity, in general, is about the accuracy, internal quality, and reliability of data [42]. Data integrity in medical records means that data should be complete, accurate, consistent, and up-to-date. In the healthcare regulatory system worldwide, data integrity refers to being complete, consistent, and accurate. It should be attributable, legible, contemporaneously recorded, original or an actual copy, and accurate, commonly referred to as "ALCOA," according to the Food and Drug Administration (FDA) [43] and the World Health Organization (WHO) [44].

This work discusses data integrity for sleep apnea patients in terms of original or authentic copies in which information came directly from patients, accurate and irreversible. It means that after the data is stored, nobody can change it.

3. Proposed sleep apnea diseases medical record

The recent works on blockchain and lightweight blockchain based on medical data records and our proposed scheme are shown in Table 2.

Liang et al. [45] proposed designing a mobile healthcare system for personal health data collection, sharing, and collaboration between individuals, healthcare providers, and insurance companies. They proposed the blockchain adopted for health data collection from healthcare providers, for personal health data access from healthcare providers and health insurance companies, to store access control policies to ensure stability.

Noh et al. [46] proposed a blockchain-based secure medical data sharing system in cloud storage. The record owners use blockchain technology to access their medical records in the cloud server without a fully trusted third party. Zheng et al. [47] proposed a conceptual design for sharing personal continuous dynamic health data using blockchain technology supplemented by cloud storage to share health-related information securely and transparently. They proposed to use blockchain to store transactional data such as the user public key, the link to the encrypted data (hash pointer), basic information, and the price of the dataset.

Fan et al. [48] proposed a blockchain-based information management system to handle patient information. They proposed the blockchain to access and retrieve electronic medical records (EMR).

Patel [49] developed a framework for cross-domain image sharing that uses a blockchain as a distributed data store to establish a ledger of radiological studies and patient-defined access permissions. The blockchain framework is shown to eliminate third-party access to protected health information, satisfy many criteria of an interoperable health system, and readily generalize to domains beyond medical imaging.

Zhu et al. [50] use the PoW consensus algorithm through the Ethereum blockchain in their proposed architecture to support data protection. Ismail et al. [51] proposed the lightweight blockchain in healthcare using PBFT consensus. Fu et al. [52] proposed privacy-preserving in healthcare blockchain systems based on lightweight message sharing.

We propose a medical record data recording scheme using a lightweight blockchain on IoT devices. In our experiment, an IoT device is attached directly to a sleep apnea patient and connected to a mobile device. Data is sent to the server for the mining process to generate the blockchain using the level of difficulty specified on the lightweight blockchain. The information is only can be read/accessed by the doctor or the families. Figure 3 shows the proposed design system.

3.1. Blockchain Structure

The blockchain structure proposed in this paper extends the Satoshi Nakamoto blockchain system by adding some details of existing block data transactions.Fig. 4 shows the blockchain structure designed to receive and record the data from the Sleep Apnea patient to the blockchain network. The blockchain structure is divided into two parts,

Table 2. Strengths and weaknesses of works on lightweight blockchain medical records.

Work	Scalability	Throughput	Blockchain	Lightweight Blockchain	IoT	Consensus
[45]	√	×	√	×	×	Proof of Integrity Proof of validation
[46]	√	×	√	×	×	Proof of Work
[47]	√	√	√	×	×	Proof of Work
[48]	√	×	√	×	×	Practical Byzantine Fault Tolerance
[49]	×	√	√	×	×	Proof of Stake
[50]	√	√	√	×	×	Proof of Work
[51]	√	√	√	√	×	Practical Byzantine Fault Tolerance
[52]	√	√	√	×	×	Proof of Work
Our proposed scheme	√	√	√	√	√	Proof of Work with Leading Zeroes

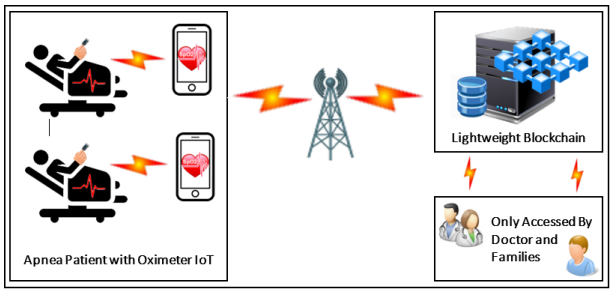

Fig. 3. The Proposed Design System.

namely the header block and transaction block. The hashing data of 256-bit is used to secure the data in the header and transaction in this proposed system.

This paper does not discuss the hashing process itself in detail. The header block contains the hashing value of the parent/previous block. If the block header is the initial block or so-called the genesis block, then the header block will contain zero hashing data because it is not related to any previous block. The transaction block contains personal data from Sleep Apnea patients, apnea medical records from the IoT (Oximeter), the hashing value of all blocks, and a timestamp for marking the block-time.

3.2. System Design

We can see the user interaction between the pulse oximeter device and the smartphone in the form of a flowchart proposed by the system in Fig. 5.

In Fig. 5, the system will ask to input the patient data and validate it. When the pulse oximeter is already turned on and is ready to send the data, the smartphone must be paired before reading the data. After successful pairing, the data from the pulse oximeter will start recording.

The data will be generated to a block in the blockchain network when we stop the recording. When another data recording is needed, then just repeat the recording process. To generate the initial or the first data from the blockchain, we need to create a block called Genesis Block. Algorithm 1 shows the algorithm for constructing the genesis block, the hash calculation, and the mining function.

The Block() procedure in Algorithm 1 is the structure of the block to be built. It consists of an Index (sequence of data), the data itself, PrevHash (data from previous Hashing data), Nonce (the number of mining iterations performed to solve a given mathematical problem), and timestamp (the date and time information when the data created). The hash value in this procedure will contain the Hash function of the data combination above.

The CalculateHashing() procedure in Algorithm 1 is used to generate the hashing value of the block. The GenerateGenesis() procedure creates an initial block with Index = 0, with Data and PrevHash values that are not yet defined or empty.The procedure that builds the next block after the genesis block is created, the mining process, the validation process, and the function for finding leading zero can be found in Algorithm 2.

The AddBlock() procedure in Algorithm 2 makes the next chain in the created block last index position. The last index position of the existing chain by calling the GetLast() function is obtainable. The Mining(Difficulty) process is to complete the mathematical problem, in this case, to find the number of leading-zero based on the hash process result. The difficulty parameter is determining how many zeros will be counted as leading-zeros and comparing them with the hash function results.

The system will recall the Hash process again by adding the current nonce value. If the results obtained are not suitable. The parameter setting for difficulty level is shown

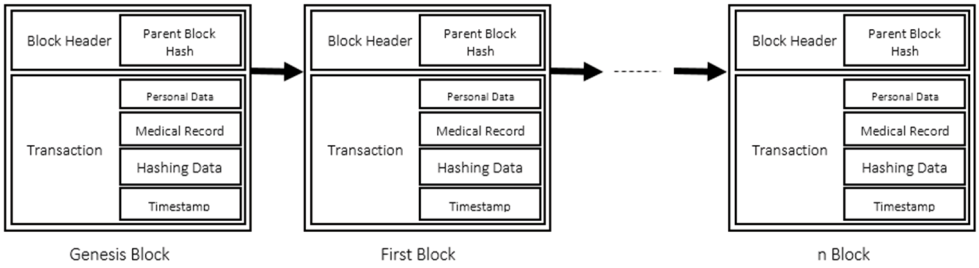

Fig. 4. Proposed Blockchain Structure.

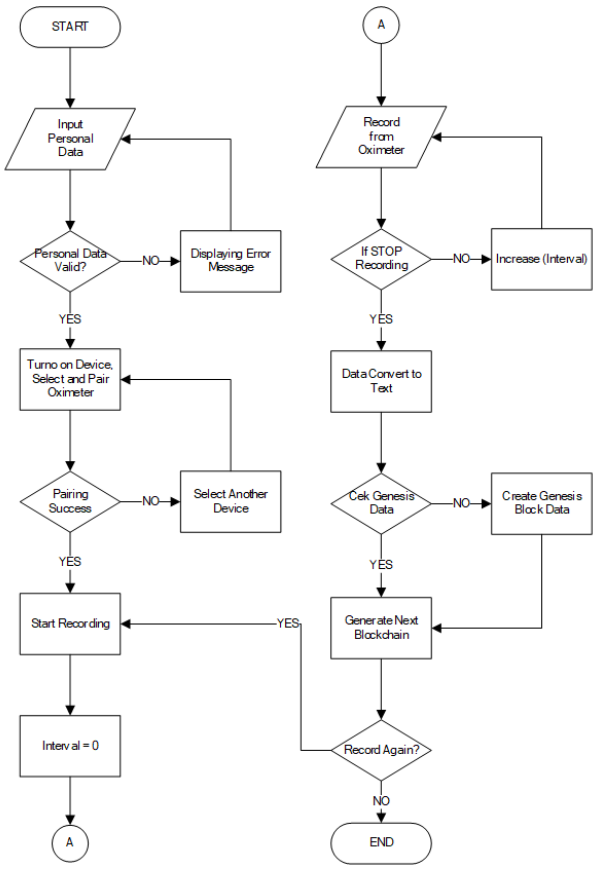

Fig. 5. Flowchart of The Proposed System.

in Table 3.

The LeadingZero() function in Algorithm 2 is a function to find the number of continuous zero (leading-zero) in the word given. It will compare the return number of this function with the difficulty parameter in the mining procedure. The counting of leading-zero will start from the most significant bit until the least significant bit.

The ValidateChainBlock() procedure is a process of validating the blocks created with the previous block. This procedure will compare the hashing value of the Current Block (CurrBlock) position with the hashing value of the Previous Block (PrevBlock). If the results are not the same, it can be sure that there is an error or damage to the data, and the block created cannot be linked, and the data is considered a mistake. The data referred to in the algorithm above is the captured data from Bluetooth Oximeter, which consists of Saturation Pulse of Oxigen (SpO2) and Beat Perminute (BPM) data from Sleep Apnea patients at a particular time.

Table 3. Difficulty Level Setting Parameter.

Difficulty Level	Number of Leading-Zeros	Example
1	1	0xxxxxxxxxx
2	2	00xxxxxxxxx
3	3	000xxxxxxxx
4	4	0000xxxxxxx
5	5	00000xxxxxx

4. Discussions

As a result, a lightweight blockchain application has been successfully designed and created to record patient medical data with Sleep Apnea symptoms using the lightweight blockchain framework. This system use Flask as a web application framework and also a lightweight web server gateway interface. Python is used to develop a blockchain program and MIT Apps Inventor as an Android application to connect with the oximeter device.

In this experiment, the difficulty level specified in Table 3 is applied to determine the mining process required to create a block. The aim is to determine the most suitable level of difficulty for this application. The same data patient identity and medical record using different difficulty levels are used to determine the time it takes during the mining process and determine how many iterations (Nonce) occur to solve a given mathematical problem. We conduct ten experiments to calculate the average iteration value of difficulty at each level. The average iteration results (Nonce) generated when making a block with the specified difficulty level can be seen in Table 4.

Algorithm 1: Generate Genesis Block

```
1.  Procedure Block(Int index, String Data, String PrevHash)
2.  Begin
3.       Me.Index ← Index
4.       Me.Data ← Data
5.       Me.PrevHash ← PrevHash
6.       Me.Nonce ← 0
7.       Me.TimeStamp ← GetDateTime(Now)
8.       Me.Hash ← Call CalculateHashing
9.  End Procedure
10.
11. Function CalculateHashing()
12. Begin
13.      CalculateHashing ← SHA265 (Me.Index + Me.PrevHash + Me.Nonce + Me. TimeStamp + Me.Data))
14. End Function
15.
16. Procedure GenerateGenesis()
17. Begin
18.      Index ← 0
19.      Data ← ""
20.      PrevHash ← ""
21.      Create New List Block (Index, Data, PrevHash, Nonce=0, TimeStamp)
22. End Procedure
23.
24. Procedure Mining(Int Difficulty)
25. Begin
26.      While Substring(0, Difficulty) <> StringRepeat(Difficulty, "0")
27.           Me.Nonce = Me.Nonce + 1
28.           Me.Hash = Call CalculateHashing
29.      End While
30. End Procedure
```

Table 4. Mining Process Duration.

Difficulty Level	Nonce/Iterate		
	Minimum	Maximum	Average
1	9	55	22.8
2	50	456	195.9
3	410	7,208	3,949.8
4	3,951	169,749	52,126.8
5	15,921	1,960,106	889,829.5

The block time it takes is also measured to create a block on the blockchain network to compare it to the existing system. The proposed block time values are compared with Bitcoin, which has a block time of 10 minutes. Ethereum, which has a block-time of 15 seconds [53], Litecoin, which has a block-time of 150 minutes. Moreover, Dogecoin, which has a block-time of 60 seconds [54, 55]. We can see the average block-time comparison results in proposed systems and existing networks when creating a block in Fig. 6.

Fig. 6 shows that the proposed block-time for a low level of difficulty has a faster duration than the existing network. At the fifth difficulty level, the required block-time appears to have a longer processing time than Ethereum. Based on Table 3 and Fig. 6, we decided to use the second difficulty level in this experiment. The reason is that the mining process is speedy and still has sufficient difficulty in making a block in the blockchain network, so it is very suitable to support IoT devices, which also require fast data processing time.

The IoT Bluetooth Oximeter device can read data on oxygen levels in the blood and BPM levels of patients with Sleep Apnea and record them into the Lightweight Blockchain framework. Users must have inserted the patient personal data before connecting the Bluetooth to the oximeter device to capture the data. After receiving the data from the Oximeter device through an android device application, it can be continued with the mining process. The mining process is complete if we notice from the system that the mining process is successful.

The hashing function in this experiment is related to data integrity. If the hashing function is applied to a transaction, it will produce a specific hashing value on all transaction data. Hence the hashing data will become the data in the following block header.

So if the data in a block is changed even only by a single character, then the hashing process results will ultimately be different from the previous. The new block data will not relate to the following block data because of the header block data difference.Therefore the data integrity on this lightweight blockchain for sleep apnea patient systems can work well and be secure.

Every data from another patient will have completely different hash data, and every information is taken from the Oximeter device also will be different because of the timestamp.The system also can display graphically based on data obtained from every Sleep Apnea patient. We use Pygal, a Python SVG Graph plotting library, to view the graphics. Data obtained from the Oximeter is oxygen saturation in the blood (SpO2) shown in Fig. 7, and the patient heart rate (BPM) shown in Fig. 8.

Algorithm 2: Generate Next Block

```
Procedure AddBlock (String Data)
Begin
      Index ← Size(Block)
      New Block(Index, Data, GetLast)
      Call Mining(Difficulty)
      Call ValidateChainBlock()
End Procedure

Function GetLast()
Begin
      GetLast ← Get(Block(Size(Block) - 1))
End Function

Procedure Mining(Difficulty)
Begin
      Nonce ← 0;
      MiningResult ← CalculateHashing()
      While length(MiningResult.LeadingZero) <> Difficulty
            Nonce ← Nonce + 1
            MiningResult ← CalculateHashing()
      End While
End Procedure

Function LeadingZero()
Begin
      If (MiningResult = 0)
            return 0
      Else
            x ← length(MiningResult)
            count ← 0
            for (i=0; i < x; i++)
                  r ← 1 << MiningResult [x-1]
                  While (MiningResult & r) = 0
                        r ← r >> 1
                        count ← count + 1
                  End While
            End For
            return count
      End If
End

Procedure ValidateChainBlock()
Begin
      For i = 1 to Size(Block) - 1
            PrevBlock ← Get(Block(Size(Block) - 1)
            CurrBlock ← Get(Block(Size(Block))
            If Hashing(CurrBlock(Hash)) <> CalculateHashing(CurrBlock) Then
                  Message("Chain Not Valid! Incorrect Current Hash!")
            Else If Hashing(CurrBlock(PrevHash)) <> Hashing(PrevBlock) Then
                  Message ("Chain Not Valid! Previous Hash not same with Previous block Hash!")
            End If
      End For
End Procedure
```

In Figs. 7 and 8, we can see the sample of graphical data taken from a single patient. The users will detect sleep apnea symptoms if their blood oxygen saturation level is below 88% or even smaller. As for the regular heart rate, it ranges between 60-100 times per minute. The two graphic images above show that the patient has no sleep apnea symptoms and has a steady heart rate.

5. Conclusions

The lightweight blockchain framework has successfully been established and tested using the sleep apnea patient data medical record. It can help record the data and ensure data recording safety from each sleep apnea patient, where data is stored wrapped using blockchain technology. The benefit of using blockchain technology is data integrity.

The user can determine the difficulty level while generating the hash function using this lightweight blockchain application. In the app, users can set the difficulty level of mining the blockchain in the configuration file.

The difficulty level tested from level one to five shows a better block-time than the existing blockchain network. It shows a higher block-time at the fifth level of difficulty than Ethereum but still faster. In this case, the difficulty level is used to find two leading-zero, which means to find the two-digit numbers in sequence at the beginning of the hash process result. A nonce is used as a counter that increases until it finds the specific hashing with two-digit leading-zeros numbers in sequence at the beginning of the resulting hashing process.

The higher the level of difficulty specified, the longer the hash function is generated. When the difficulty level is determined to be level five in the experiment, the hash function obtained takes approximately one to two minutes. The more extended development of this hash function could

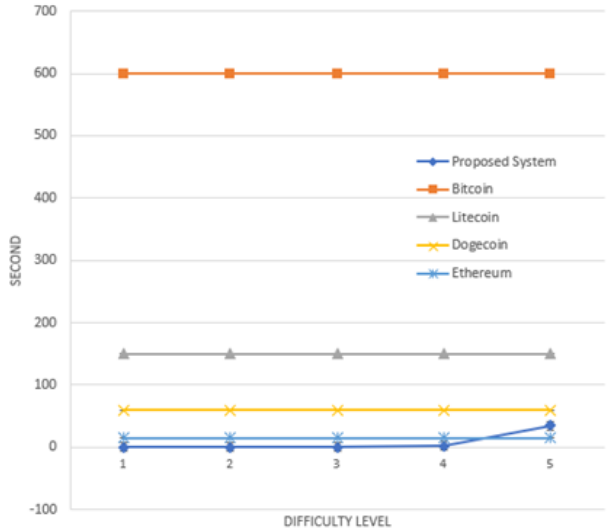

Fig. 6. Block-Time Average in Proposed Systems and Actual Network.

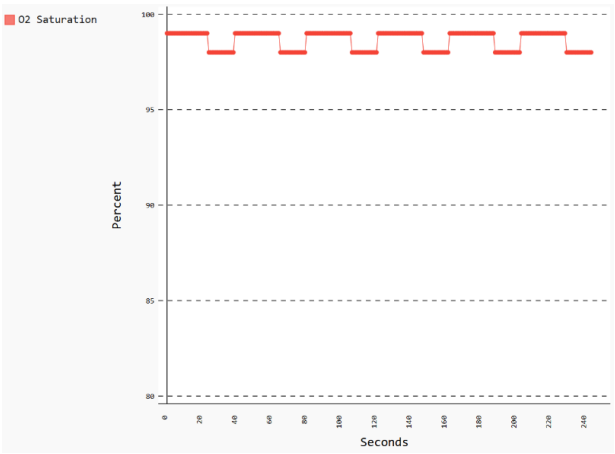

Fig. 7. Oxygen Saturation Data.

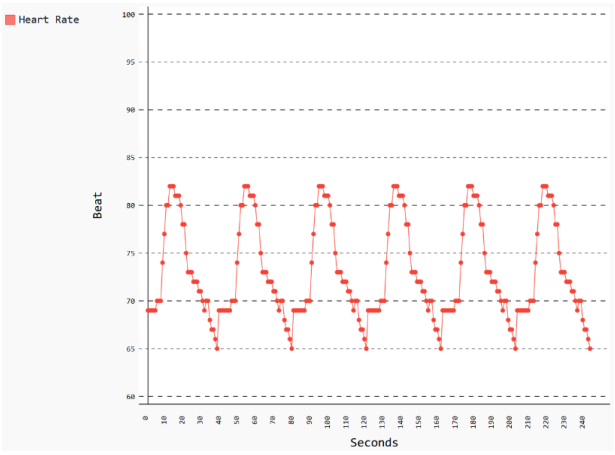

Fig. 8. Heart Rate Data.

have caused a connection loss when it caused the data to be inadequately processed.

In the future, a lightweight blockchain framework can still be developed by adding artificial intelligence to ensure that the data comes from the right patient and adapt the IoT environment to determine the difficulty levels that suit the systems. The type of IoT device used as reference data in data transactions can also improve data integrity. Because each IoT product has a different Product ID, this can be used to identify a single device that connects to a single patient.

Acknowledgments

We would like to thank the University of Indonesia for providing financial assistance under the research scheme of PUTI DOKTOR, grant number NKB-685/UN2.RST/HKP.05.00/2020.

References

[1] M. Mettler. "Blockchain technology in healthcare: The revolution starts here". In: *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 1–3. DOI: https://doi.org/10.1109/HealthCom.2016.7749510.

[2] G. Hasenstab. *Three Ways Blockchain Is Improving Our Lives Now*. 2019. URL: https://www.forbes.com/sites/forbesrealestatecouncil/2019/12/02/three-ways-blockchain-is-improving-our-lives-now/?sh=201ba3894572.

[3] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, (2020) *"Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare"* **Electronics** *9*(10): DOI: https://doi.org/10.3390/electronics9101609.

[4] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman. *A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data — MIT Media Lab*. 2016. URL: https://www.media.mit.edu/publications/medrec-whitepaper/.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management". In: *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. DOI: https://doi.org/10.1109/OBD.2016.11.

[6] J. Zhang and M. Wu, (2020) *"Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine"* **Electronics** *9*(10): DOI: https://doi.org/10.3390/electronics9101746.

[7] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home". In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623. DOI: https://doi.org/10.1109/PERCOMW.2017.7917634.

[8] Y. Zhang and J. Wen, (2017) *"The IoT electric business model: Using blockchain technology for the internet of things"* **Peer-To-Peer Networking and Applications *10***(4): 983–994. DOI: http://dx.doi.org/10.1007/s12083-016-0456-1.

[9] H. Tan, P. Kim, and I. Chung, (2020) *"Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pandemic Control"* **Electronics *9***(10): DOI: https://doi.org/10.3390/electronics9101683.

[10] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, (2020) *"A Review of Blockchain-Based Systems in Transportation"* **Information *11***(1): DOI: https://doi.org/10.3390/info11010021.

[11] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko, (2020) *"Technological Aspects of Blockchain Application for Vehicle-to-Network"* **Information *11***(10): DOI: https://doi.org/10.3390/info11100465.

[12] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, (2016) *"Internet of Things, Blockchain and Shared Economy Applications"* **Procedia Computer Science *98***: 461–466. DOI: https://doi.org/10.1016/j.procs.2016.09.074.

[13] P. Hurich, (2016) *"The Virtual is Real: An Argument for Characterizing Bitcoins as Private Property"* **Banking & Finance Law Review *31***(3): 573–583.

[14] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen. "The Blockchain as a Software Connector". In: *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, 182–191. DOI: https://doi.org/10.1109/WICSA.2016.21.

[15] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, (2018) *"Decentralized Applications: The Blockchain-Empowered Software System"* **IEEE Access *6***: 53019–53033. DOI: https://doi.org/10.1109/ACCESS.2018.2870644.

[16] N. Kshetri and J. Voas, (2018) *"Blockchain-Enabled E-Voting"* **IEEE Software *35***(4): 95–99. DOI: https://doi.org/10.1109/MS.2018.2801546.

[17] C.-k. Chang, (2020) *"Blockchain for Integrated Nuclear Power Plants Management System"* **Information *11***(6): DOI: https://doi.org/10.3390/info11060282.

[18] S. Nakamoto, (2009) *"Bitcoin: A Peer-to-Peer Electronic Cash System"*:

[19] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, (2019) *"FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing"* **Journal of Systems and Software *154***: 22–36. DOI: https://doi.org/10.1016/j.jss.2019.04.050.

[20] J. Zhang, N. Xue, and X. Huang, (2016) *"A Secure System For Pervasive Social Network-Based Healthcare"* **IEEE Access *4***: 9239–9250. DOI: https://doi.org/10.1109/ACCESS.2016.2645904.

[21] N. Jia, R. Wang, M. Li, Y. Guan, and F. Zhou, (2021) *"Towards the Concurrent Optimization of the Server: A Case Study on Sport Health Simulation"* **Complexity *2021***: 5587170. DOI: https://doi.org/10.1155/2021/5587170.

[22] T. Bizimungu, D. Harelimana, and J. Marie Ntaganda, *"A Client-Server and Web-Based Graphical User Interface Design for the Mathematical Model of Cardiovascular-Respiratory System"* **Applied Computational Intelligence and Soft Computing *2021***: 5581937. DOI: https://doi.org/10.1155/2021/5581937.

[23] L. Ibraimi, M. Asim, and M. Petković. "Secure management of personal health records by applying attribute-based encryption". In: *Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health*, 71–74. DOI: https://doi.org/10.1109/PHEALTH.2009.5754828.

[24] M. A. Sarwar, T. Bashir, O. Shahzad, and A. Abbas, (2019) *"Cloud-Based Architecture to Implement Electronic Health Record (EHR) System in Pakistan"* **IT Professional *21***(3): 49–54. DOI: https://doi.org/10.1109/MITP.2018.2882437.

[25] X. Yan and X. Ren, *"5G Edge Computing Enabled Directional Data Collection for Medical Community Electronic Health Records"* **Journal of Healthcare Engineering *2021***: 5598077. DOI: https://doi.org/10.1155/2021/5598077.

[26] D. D. L. F. Simon Fernandez-Vazquez Rafael Rosillo and P. Priore, (2019) *"Blockchain in FinTech: A Mapping Study"* **Sustainability MDPI *11***(22): DOI: https://doi.org/10.3390/su11226366.

[27] E. A. A. Lukman Adewale Ajao James Agajo and L. Karngong, (2019) *"Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry"* **Multidisciplinary Scientific Journal - MDPI 2**(3): 300–325.

[28] C. Arnold, D. Kiel, and K.-I. Voigt, (2016) *"How The Industrial Internet of Things Changes Business Models in Different Manufacturing Industries"* **International Journal of Innovation Management *20***(08): 1640015. DOI: https://doi.org/10.1142/S1363919616400156.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". In: *2015 IEEE Symposium on Security and Privacy*, 104–121. DOI: https://doi.org/10.1109/SP.2015.14.

[30] L. Cocco and M. Marchesi, (2016) *"Modeling and Simulation of the Economics of Mining in the Bitcoin Market"* **PLOS ONE *11***: DOI: https://doi.org/10.1371/journal.pone.0164603.

[31] S. Javaheri, F. Barbe, F. Campos-Rodriguez, J. A. Dempsey, R. Khayat, S. Javaheri, A. Malhotra, M. A. Martinez-Garcia, R. Mehra, A. I. Pack, V. Y. Polotsky, S. Redline, and V. K. Somers, (2017) *"Sleep Apnea"* **Journal of the American College of Cardiology *69***(7): 841. DOI: https://doi.org/10.1016/j.jacc.2016.11.069.

[32] W. Su, G. Chen, D. Ma, J. Zeng, F. Yan, X. Lin, Z. Xu, S. Yang, Z. Li, and C. Liu, *"Higher Apnea-Hypopnea Index (AHI) and Oxygen Desaturation Index (ODI) Were Independently Associated with Increased Risks of Hypertension in Patients with T2DM: A Cross-Sectional Study"* **International Journal of Hypertension *2021***: 8887944. DOI: https://doi.org/10.1155/2021/8887944.

[33] T. Saunamäki, E. Huupponen, J. Loponen, and S.-L. Himanen, (2017) *"CPAP Treatment Partly Normalizes Sleep Spindle Features in Obstructive Sleep Apnea"* **Sleep Disorders *2017***: 2962479. DOI: https://doi.org/10.1155/2017/2962479.

[34] AASM, (2008) *"Obstructive Sleep Apnea"* ***2019***(December 13):

[35] S. Shankar, S. S. Gupta, G. Rojas-Marte, S. Demir, A. Saxena, C. Obiagwu, N. Aggarwal, A. K. Rai, S. Kamholz, V. Shetty, and Y. Kupfer, (2019) *"Electrocardiographic Associations Seen with Obstructive Sleep Apnea"* **Sleep Disorders *2019***: 9704785. DOI: https://doi.org/10.1155/2019/9704785.

[36] A. Manoni, F. Loreti, V. Radicioni, D. Pellegrino, L. Della Torre, A. Gumiero, D. Halicki, P. Palange, and F. Irrera, (2020) *"A New Wearable System for Home Sleep Apnea Testing, Screening, and Classification"* **Sensors *20***(24): DOI: https://doi.org/10.3390/s20247014.

[37] C. Esteban-Amarilla, S. Martin-Bote, A. Jurado-Garcia, A. Palomares-Muriana, N. Feu-Collado, and B. Jurado-Gamez, *"Usefulness of Home Overnight Pulse Oximetry in Patients with Suspected Sleep-Disordered Breathing"* **Canadian Respiratory Journal *2020***: 1891285. DOI: https://doi.org/10.1155/2020/1891285.

[38] S. Shah, K. Majmudar, A. Stein, N. Gupta, S. Suppes, M. Karamanis, J. Capannari, S. Sethi, and C. Patte, (2020) *"Novel Use of Home Pulse Oximetry Monitoring in COVID-19 Patients Discharged From the Emergency Department Identifies Need for Hospitalization"* **Academic Emergency Medicine *27***(8): 681–692. DOI: https://doi.org/10.1111/acem.14053.

[39] A. Von Chong, M. Terosiet, A. Histace, and O. Romain, (2019) *"Towards a novel single-LED pulse oximeter based on a multispectral sensor for IoT applications"* **Microelectronics Journal *88***: 128–136. DOI: https://doi.org/10.1016/j.mejo.2018.03.005.

[40] MIT and Google. *MIT App Inventor | Explore MIT App Inventor*. 2010. URL: http://appinventor.mit.edu/.

[41] B. Xie and H. Abelson. "Skill progression in MIT app inventor". In: *2016 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, 213–217. DOI: https://doi.org/10.1109/VLHCC.2016.7739687.

[42] P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, and F. Whittaker. "Ensuring Data Integrity in Electronic Health Records: A Quality Health Care Implication". In: *International Conference on Orange Technologies*. DOI: https://doi.org/10.1109/ICOT.2016.8278970.

[43] A. K. Rattan, (2018) *"Data Integrity: History, Issues, and Remediation of Issues"* **PDA J Pharm Sci Technol *72***(2): 105–116. DOI: https://doi.org/10.5731/pdajpst.2017.007765.

[44] WHO, (2014) *"Annex 5 Guidance on good data and record management practices"*:

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

[46] S.-W. Noh, Y. Park, C. Sur, S.-U. Shin, and K.-H. Rhee, (2017) *"Blockchain-Based User-Centric Records Management System"* **International Journal of Control and Automation *10***: 133–144. DOI: https://dx.doi.org/10.14257/ijca.2017.10.11.12.

[47] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere. "Blockchain-based Personal Health Data Sharing System Using Cloud Storage". In: *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 1–6. DOI: https://doi.org/10.1109/HealthCom.2018.8531125.

[48] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, (2018) *"MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain"* **Journal of Medical Systems *42***(8): 1–11. DOI: https://dx.doi.org/10.1007/s10916-018-0993-7.

[49] V. Patel, (2018) *"A framework for secure and decentralized sharing of medical imaging data via blockchain consensus"* **Health Informatics Journal *25***(4): 1398–1411. DOI: https://doi.org/10.1177/1460458218769699.

[50] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, (2019) *"Controllable and trustworthy blockchain-based cloud data management"* **Future Generation Computer Systems *91***: 527–535. DOI: https://doi.org/10.1016/j.future.2018.09.019.

[51] L. Ismail, H. Materwala, and S. Zeadally, (2019) *"Lightweight Blockchain for Healthcare"* **IEEE Access *7***: 149935–149951. DOI: https://doi.org/10.1109/ACCESS.2019.2947613.

[52] J. Fu, N. Wang, and Y. Cai, (2020) *"Sensor Research; New Sensor Research Study Findings Recently Were Reported by Researchers at Beijing University of Posts and Telecommunications (Privacy-Preserving in Healthcare Blockchain Systems Based on Lightweight Message Sharing)"* **Health & Medicine Week**: 3596.

[53] J. Chiu and T. V. Koeppl, (2019) *"Blockchain-Based Settlement for Asset Trading"* **The Review of Financial Studies *32***(5): 1716–1753. DOI: https://doi.org/10.1093/rfs/hhy122.

[54] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo. "SimBlock: A Blockchain Network Simulator". In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 325–329. DOI: https://doi.org/10.1109/INFCOMW.2019.8845253.

[55] U. W. Chohan, (2017) *"A History of Dogecoin"*: DOI: http://dx.doi.org/10.2139/ssrn.3091219.