information

MDPI

Article

Secure Medical Blockchain Model

Ibrahim Shawky Farahat [1,*], Waleed Aladrousy [1], Mohamed Elhoseny [1,2], Samir Elmougy [1] and Ahmed Elsaid Tolba [1,3]

[1] Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[2] College of Computing and Informatics, University of Sharjah, Sharjah 272722, United Arab Emirates
[3] The Higher Institute of Engineering and Automotive Technology and Energy, New Heliopolis 11829, Egypt
* Correspondence: ishawky@fci.luxor.edu.eg

Abstract: The Internet of Medical Things (IoMT) uses wireless networks to help patients to communicate with healthcare professionals. Therefore, IoMT devices suffer from a lack of security controls, just like many Internet of Things (IoT) gadgets. Thus, in this paper, we develop a system that uses a blockchain to secure medical data for each transaction between physicians and patients. This system also helps the physician to send the treatment to the blockchain. The blockchain creates a new block for the treatment and connects it with the previous block. This system also helps patients to access their treatment through the blockchain. SHA-256 is used to hash the new block using some information about the last block. We modify SHA-256 using the LZ4 algorithm to compress data. We also prevent a new block hash code starting with a specific number of zeros, which made the proposed system give a time complexity better than all related work. In this paper, we also develop a party-authentication technique that ensures the two parties of the transaction. The proposed system makes a transaction with O(n) time complexity. Thus, our system takes 1 s to create a block for the transaction. We also make a green computing algorithm comparison between our proposed system and the blockchain version. This comparison proves that our proposed method consumes less energy to create a new block. This paper proves that our method performs better than all previous blockchain versions.

Keywords: security; blockchain; privacy; compression; SHA-256; hashing; LZ4

check for updates

Citation: Farahat, I.S.; Aladrousy, W.; Elhoseny, M.; Elmougy, S.; Tolba, A.E. Secure Medical Blockchain Model. *Information* **2023**, *14*, 80. https://doi.org/10.3390/info14020080

Academic Editor: Nelly Leligou

Received: 4 December 2022
Revised: 15 January 2023
Accepted: 27 January 2023
Published: 30 January 2023

1. Introduction

Internet of Things (IoT) was valued at USD113.75 billion in 2019 in the healthcare field [1]. IoT is also expected to reach a net worth of USD332.67 billion by 2027 due to its rapid growth [2]. Nowadays, digital hospitals use hundreds of linked devices, such as wearables, monitors, workflow, imaging, and patient data systems, as well as implants and other medical equipment. These touchpoints have several benefits for improving patient care, but many medical IoT devices lack strong security and might be used as a gateway to the hospital's network. In-home telehealth medical equipment, such as those used to track a patient's blood pressure or blood sugar, is another possible weak point. The hospital's system is momentarily exposed to a cyberattack when the information is wirelessly transmitted to healthcare providers over an unencrypted Wi-Fi connection or the public internet [3]. Hence, the most important issue confronting the healthcare sector right now is data security. Medical institutions are obvious targets since they handle enormous volumes of sensitive patient data, and many do not have the knowledge and resources to do so. In the last several years, healthcare has carried out many achievements. These achievements allow many patients to access their medical histories and test results through online portals [4]. Vital signs transfer from patient to doctor across the IoT network, making it simple for doctors to keep track of their patients. Thus, these data are vulnerable to network attacks from hackers, who can alter or steal them. Therefore, IoT faces a significant challenge in protecting these data. According to [5], Table 1 outlines the security issues that IoT may face.

Table 1. Security problems that face IoT [5].

Security Problem	Percentage
Inadequate authentication	80%
Privacy issues	90%
Plaintext communication	70%

Table 1 shows that medical data face three problems. These three problems happened because medical data can be hacked when they are sent from patient to doctor. Hence, there is a need for a technique that protects these data. Many technologies have been developed in recent years to safeguard and preserve sensitive medical data. Some of the linked papers advise centrally storing medical data [6]. These methods face two issues when they are used to protect medical data. The first issue is there is not enough room to store the medical data. How to protect data from unwanted access is the other issue. As a result, many scientists use decentralized storage to protect these data [7]. Furthermore, they suggest that the blockchain is the best mechanism for keeping such data since hacking requires changing all blocks. As a result, it is difficult to hack systems that use numerous blocks to store data. Obtaining any information is made harder yet by hashing the new block with the transactional information and commencing the hash with the fixed number zero. The blockchain will quickly detect any changes to a single block without affecting all the preceding blocks, ensuring that the data are safe.

In this paper, we develop a system that enables patients to receive their therapy without seeing a doctor. Vital signs of the patient are collected by the IoT system that we implemented before [8]. After that, the patients send vital signs through the internet. Additionally, the doctor uses the internet to mail the patient's medication. The proposed system is divided into two primary components. The first component is using blockchain to store the information of each transaction. Each transaction is stored as a new block and connected with the last block using a specific hash function. We modify the SHA-256 hash function to hash new blocks using the LZ4 algorithm to compress the information. As a result, the time needed to create a block will be reduced. The second component involves checking the authentication between the two parties of the transaction. Thus, the objectives of our paper are:

1. Implement a medical blockchain model using the Ethereum blockchain platform.
2. Modify the Ethereum blockchain using SHA-256 as a hash function.
3. Modify the SHA-256 hash algorithm using the LZ4 algorithm to speed up the process of creating blocks.
4. Modify the SHA-256 hash algorithm by preventing the hash code from starting with 0 to speed up the process of creating blocks.
5. Implement a party-authentication technique to complete transactions after verifying the patient and doctor's identities.

The structure of this paper is as follows: Section 2 discusses some background and related work, Section 3 presents the proposed work, Section 4 presents the experiments and their results, and Section 5 introduces the conclusion of the paper.

2. Background and Related Work

Blockchain represents each transaction in the form of a block, so a blockchain appears as a chain of blocks [9]. Besides the information about the transaction, the new block holds additional information such as the block number, block time creation, and block hashing. The idea of the blockchain came from connecting the new block with the previous block. The created block uses a hash function to hash the transaction information with the previous block hash [10]. Therefore, the blockchain appears as a chain of connected blocks.

Hence, if any hacker wants to track or sniff the transaction information, they must hack all previous blocks. A blockchain forbids the use of third-party intermediaries [11]. For instance, banks are not permitted to interfere with money transfers. Figure 1 shows that the blockchain appears as a chain of connected blocks.

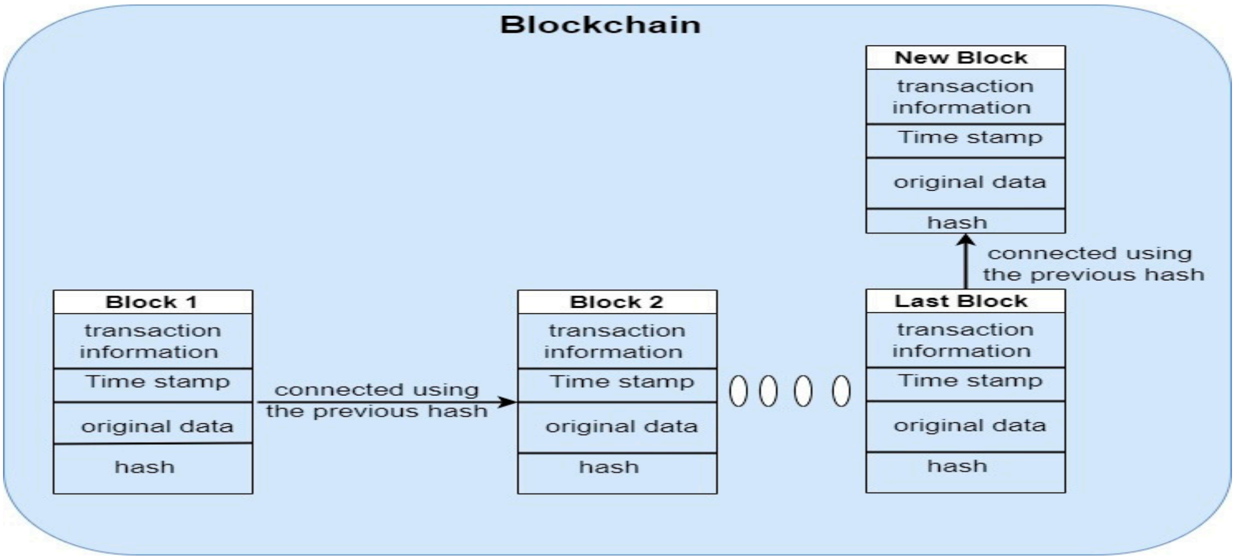

Figure 1. Blockchain blocks.

Blockchain has three different versions [12]. Blockchain Version 1.0 is built to secure cryptocurrency and was released in 2005 by Hall Finley. Blockchain Version 1.0 uses Distributed Ledger Technology (DLT), which makes blockchain protect financial transactions and is carried out with the aid of bitcoin. However, this version lacks restrictions since any user may complete any bitcoin transaction. Blockchain Version 1.0 is utilized in payments and digital currency [13]. Version 1.0 of blockchain had a flaw in that mining bitcoin was wasteful and was not scalable, which led to the release of the updated version. Therefore, blockchain Version 2.0 was improved to solve the problems of blockchain Version 1.0. This version of the blockchain supports smart contracts and simple cryptocurrencies. Small contracts are hence little computers that reside in chains of blocks. These little computers run free software that automatically checks the earlier established conditions, such as facilitation, verification, or enforcement, and lowers transaction costs. Ethereum has supplanted bitcoin in blockchain Version 2.0 [14]. As a result, blockchain Version 2.0 processed many transactions quickly on the public network.

Blockchain Version 3.0 is based on features called Decentralized Apps (DApps). A DApp is similar to a regular app in that it may have a frontend written in any language that calls its backend, and that code runs on a decentralized peer-to-peer network in the backend. It uses decentralized communication and storage methods, such as Ethereum Swarm. Numerous decentralized applications exist, including BitMessage, BitTorrent, Tor, and Popcorn [15]. Nowadays, many blockchain platforms have appeared. Thus many researchers have started to discuss the role of the blockchain and make a comparison between the platforms. For example, Ratta et al. [16] discussed the role of using blockchain versions of IoT technology to improve healthcare applications. The authors showed that they could use IoT and blockchain in the healthcare system in three key areas: remote patient monitoring, medication traceability, and medical record management. They also mention the difficulties that face IoT and blockchain in healthcare systems.

Macdonald et al. [17] discussed how the blockchain could use bitcoin. They also compared Ethereum, IBM Open Blockchain, Intel Sawtooth Lake, Blockstream Sidechain Elements, and Eris blockchain platforms based on many factors, such as usability, scalability, security, and feasibility. Their comparison showed that Ethereum is the best-suited one.

Yu et al. [18] carried out a practical comparison between Ethereum, Hyperledger Fabric, and MultiChain blockchain platforms. Their comparison is limited to the blockchain methods that contain a smart contract system. This comparison showed that the implemented application determines the best platform to use (e.g., maintenance for Ethereum, fine-grained access control for Hyperledger Fabric, and rapid development for MultiChain). The authors also suggested using blockchain technology in the biomedical and healthcare sectors to reduce the probability of data theft.

Chowdhury et al. [19] presented a comparative analysis of various blockchain platforms. The authors compared 11 blockchain platforms. They used quantitative and qualitative analysis to help developers choose the best blockchain platform. The results of their analysis prove that Hyperledger Burrow lacks comprehensive documentation. As a result, the authors advised against using it. Their results also show that the Fabric platform was robust and that Sawtooth offered the best level of security.

Furthermore, many scientists have developed a blockchain-based security system based on one of the blockchain versions. Rupa et al. [20] proposed an IoT system that monitors and manages the automated vehicle. They developed a blockchain system to secure and store the data collected from the IoT system. They created a new block to store the data, then used the SHA-1 algorithm to hash the new block and connected it with the previous block.

Bigini et al. [21] identified the importance of using blockchain in IoT applications. They also provided summaries of studies and reports that aimed to assess the state of the market and pinpoint challenges for adopting a user-centric development strategy. Mohanta et al. [22] presented a comprehensive analysis of the numerous applications of blockchain technology. Additionally, they discussed the difficulties in implementing blockchain and the related security and privacy concerns. Li et al. [23] developed a mechanism to securely and effectively transfer prescription histories among various healthcare organizations. In the Decentralized Medication Management System (DMMS), a doctor evaluates the patient and issues a prescription. No one can access the patient's record without the patient's private key because the prescription is encrypted with the patient's public key. In addition to the doctor viewing the patient's record with the patient's consent, the patient can view their record. Ktari et al. [24] offered a platform built on IoT that enables patient health monitoring. They employed blockchain as a safe method to secure patient data. They collected medical data from several intelligent sensors, including blood pressure, SPO2 levels, and EEG signals. These data were collected with a Raspberry PI 4 embedded platform that served as a smart data relay, processed on a backend server, and finally saved in a Blockchain embedded node. The preliminary findings demonstrated the platform's efficacy as a potential low-cost example of a protected electronic health record (EHR). Ibrar et al. [25] used blockchain smart contracts to provide a controlled response to the needs of patients, doctors, and healthcare providers. They used blockchain to share health data among blockchain users. The Modified Merkle Tree data structure was also used to hash new blocks. The blockchain serves as a clinical data repository in this system, giving patients easy access to their electronic health records through healthcare providers. A distributed ledger that records all occurrences details is used. Through the use of cryptographic hash algorithms, this system offers great security and integrity. The effectiveness of the suggested approach has been tested through several trials. Khatoon [26] presents recent studies about blockchain-based healthcare applications and several blockchain-based processes for the healthcare industry to improve data management. Several medical data, including challenging surgical and clinical trial procedures, have been developed and implemented using the Ethereum blockchain platform. A feasibility study was conducted to determine the cost of implementing the smart medical contract system's workflows for managing healthcare. This paper presents lowering the cost of healthcare services. Because the author uses smart contracts with blockchain, this paper uses blockchain version 2.0. Baiju et al. [27] used blockchain version 2.0 with the Ethereum blockchain. Truffle served as a building block for the system. Smart contracts managed electronic medical records. These contracts track the transactions and computations that occur inside the system. They modified the smart contracts to make them workable since medical information differs from the resources utilized with blockchains, such as bitcoins and NFTs. They saved the data using the DApp wallet address, and it was required to access them to make changes to the patient's data. An operational logistic regression model receives the data as input and tunnels it over the API to analyze it to determine the patient's health state. The model then calculates the results and gives the data to the user. Mehbodniya et al. [28] developed a security framework based on the blockchain model. The authors used a modified Lamport Merkle digital signature technique to hash a new block. They used a central healthcare controller (CHC) to perform authentication and verification as well as know who created the signature. The signature must be verified using the validation hash of the public key and the create key. Their results showed that their proposed method is more effective, affordable, and quick.

In [29] we proposed a pervious blockchain and master contract system. In this system, we use blockchain to store the medical data of the patient and master contract to guarantee sending the money to the doctor after they send the treatment. We connect the last block with the new block by hashing the medical data of the new transaction with the last block hash code. We carry this out using the SHA-256 algorithm and use run length code to compress the data. This system takes O(n + d) time complexity to create a new block.

There are some recent studies that built a blockchain system with the aid of a DL learning algorithm. For example, Kumar et al. [30] developed a security system using blockchain and a DL algorithm. They used an Ethereum blockchain model to store the medical data, Stacked Sparse Variational Autoencoder (SSVA) algorithm to transform the medical data into any form readable by the computer, and the Self-Attention-Based Bidirectional Long Short-term memory (SABBLS) algorithm to detect any attack type. They used IoT-Botnet and TON-IoT datasets to ensure the security of their system. The results show that their method performed better than all previous methods.

All current works contain several flaws. They based their approach on the Ethereum blockchain without any modification to it. As a result, creating blocks requires extra time in their system. Additionally, they developed their security mechanism without requiring authentication of the two parties to the transaction. As a result, hackers could be able to impersonate patients or doctors.

3. Secure Blockchain Model

The proposed method consists of two parts. The first part implements a blockchain that creates a new block by hashing the transaction information and the previous block hash. Our blockchain uses SHA-256 to hash the new block. The second part of the system is to implement a new technique to check the authentication between the two parties. Figure 2 shows the framework of the proposed method. This figure shows that we used a previously developed IoMT system that we implemented before [8]. Figure 2 shows that our IoMT system measures vital signs. Then microcontroller sends them to the blockchain. Next, a blockchain starts to create a new block. We connected the new block by using the last block hash. Then the blockchain checks the two parties of the transaction. This check is conducted by asking the patient and physician to send their hash codes. After the blockchain receives the two parties' hash codes, it compares the two hashes with the hash code that it generates. Then, the physician can access the patient vital signs through the blockchain. When the physician sends the treatment, the blockchain creates a new block of the treatment and has the new block with the last block.

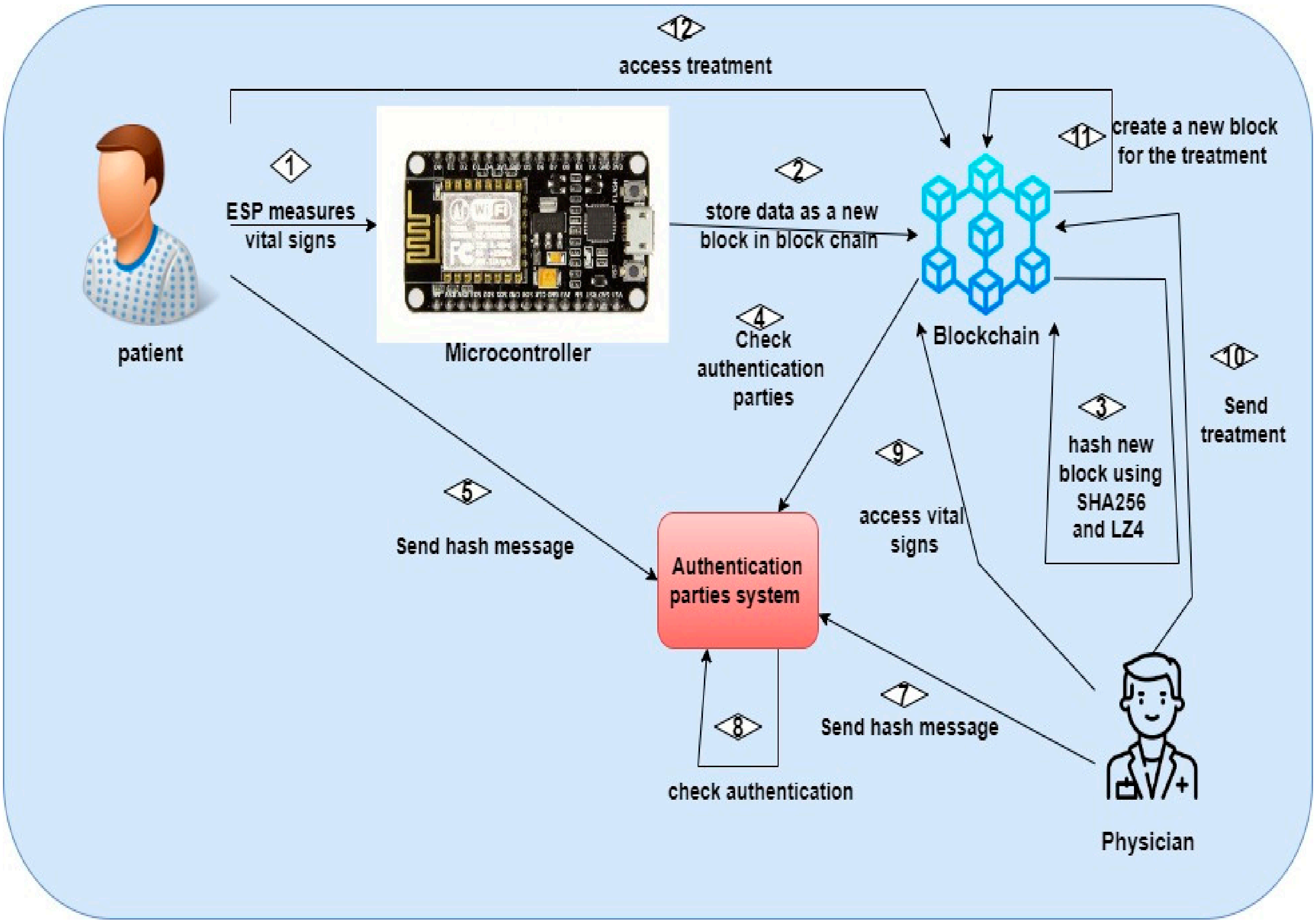

Figure 2. Framework of the proposed system.

To design our blockchain, we first need to establish what a block is because a blockchain is made up of them. The main piece of information stored in a blockchain is a block. Blocks are stored securely using the blockchain as its primary function. The letters Bl designate a generic block. When there is a transaction between two entities, a block is formed. Block $\mathrm{Bl_f}$ may be defined as follows since it has several entries (D) of size M:

$$\mathrm{Bl_f} = (\mathrm{D1}, \ldots, \ \mathrm{DN}) \tag{1}$$

where D is the entries inside the block. A link between two blocks is established using a mathematical conundrum known as the proof of work. The header of the second block is where this link will show up. A miner is someone who is looking for evidence of their effort. Let us imagine two blocks, Bprev and Bnew, together with an amount known as bits and denoted by the letter t. A goal number can be generated right away from the value of t, which expresses how difficult the proof of work is. This target is a 64-digit hexadecimal number, where the leftmost digits are largely zeros, such as:

00iqwe1234kjugfwr785621vu4abpot23r40a78sfasdasdcvfreqfghy45621ab40.

We employ the Sha-256 hashing function algorithm on the blockchain. After assuming that we are aware of the hash of the block before it, SHA(Bl_i), we will define the hash of a specific block. The formula we use to determine the new block's hashing is given by:

$$\mathrm{SHA}(Bl_{new}) = \mathrm{SHA}(\mathrm{SHA}(Bl_i\ ) \ \oplus \ stamp(t) \oplus \ t \ \oplus \ nonce) \leq \ target \tag{2}$$

where *stamp*(*t*) stands for the present time and ⊕ stands for the concatenation operation. Using the aforementioned notations, we may provide block *Bl*'s header after the proof of work for blocks (*Bl*$_i$, *Bl*) has been resolved:

$$Heading(Bnew) = \left(i_m,\ SHA\left(B_p\ \right),\ stamp(t),\ t\ ,\ nonce\ ,\ SHA(Bl_{new})\right) \tag{3}$$

where i_m is the transaction information. We design a new algorithm, Algorithm 1, to describe the role that our blockchain plays. Table 2 shows the notations that are used in all algorithms in this work.

Algorithm 1 The proposed medical blockchain

```
Input: $VS_i$ AD( $P_i$), AD($D_i$))
Output: $Hcode_i$
Begin
    $M_C$ sends $VS_i$ of $P_i$ to the $B_s$
$B_s$ uses $SHA_{256}$ to compute $Hcode_{new}$ using   $VS_i$ and $Hcode_{i-1}$.
$B_s$ creates a $NB_i$ by adding $VS_i$, $Ts_i$, and       $Hcode_{new}$.
$B_s$ add $NB_i$ to the chain and connects it to       $NB_{i-1}$ using $Hcode_{i-1}$.
x = Checkparties(AD( $P_i$), ad($D_i$))
If x== true
$D_i$ access $VS_i$ of  $P_i$ through $B_s$
$D_i$ sends treatment to $B_s$
            $B_s$ uses $SHA_{256}$ to compute $Hcode_{new}$ using  $TR_i$ and $Hcode_{i-1}$.
            $B_s$ creates a $NB_i$ by adding
               $TR_i$, $Ts_i$, and   $Hcode_{new}$.
 $P_i$ sees $TR_i$ through $B_s$
End
     End
```

Table 2. Different notations and their meaning used in this wok.

NOTATION	MEANING
M_c	Microcontroller (ESP8266)
VS_i	Vital signs
P_i	Patient
B_s	Medical Blockchain
SHA_{256}	Modified SHA-256
NB_i	New block
$Hcode_i$	Hash of block i
Ts_i	Time stamp
TI_i	transaction information
D_i	Doctor
TR_i	Treatment
AD	Wallet Address

Algorithm 1 presents that our developed IoMT system developed in [8] measures the patient vital signs and sends them to the blockchain system. Our blockchain system creates a new block by adding vital signs and hashing the code of the new block. The hash code of the new block is calculated using the last block's hash code and the vital signs of the new block. Finally, the blockchain checks the authentication of the transaction parties. If the two users are authenticated, the physician obtains permission to see the patient's vital signs and can then send the treatment to the blockchain system.

The blockchain starts to create a new block to store the treatment. Blockchain connects the new block with the last block by hashing the treatment information with the last block hash code. Finally, blockchain gives access to the patient to see treatment.

We use the SHA-256 algorithm to obtain the hashing code of the new block. We also use the hashing code to connect the new block with the last block. Algorithm 2 presents the modified SHA-256 algorithm used in this work, which is needed to convert vital signs and the last block hash into ASCII form. Therefore, we divide the data into blocks. Each block consists of 512 characters. If the last block does not contain 512 characters, then we expand it with 0 characters to make it 512 characters. Therefore, we use the LZ4 algorithm to compress the data.

Algorithm 2 The modified SHA-265 algorithm

```
SHA-256( $VS_i$, $Hcode_i$)

input: $VS_i$ and $Hcode_i$
 output: hashing function
begin
      O=concatenate ($VS_i$, $Hcode_i$)
      ascii_data $\rightarrow$ ASCII(O).
      X = size(ascii_data) /512
      For i = 1 to X
              For j = 1:512
              If i == 1
                B[i][j] = ascii_data[j]
              else
                K = j + 512*i;
                B[i][j] = ascii_data[k]
              End
          End
   End
Ifsize( B[lastrow]) < 512,
    For i = size( B[lastrow]: 512
                B[ size( B[lastrow]][j] = 0
    End.
For i = 0:64
   H = LZ4(B)
End
Return Hashing.
End
```

Algorithm 2 shows that the new block hash code does not start with a specific number of zeros. This step makes our algorithm perform faster than usual.

The second part of our system is to check the authentication of parties between the patient and the client. Thus, in this paper, we also implemented a party-authentication technique. In this technique, we use our modified SHA-256 hashing function.

We implement this technique in our blockchain system. The blockchain combines the two addresses (patient and doctor) and specific words, for example, the hello word. Then it hashes them using a modified SHA-256 algorithm. The doctor and patient devices also start to combine the address of the patient and doctor's wallets and add the hello word to them. Next, they hash it using the modified SHA-256 algorithm. After that, they send their hashing code to the blockchain. Then, the blockchain compares the received hash with the hash that it creates. If it is equal, the blockchain trusts the two devices and starts to perform its work. Otherwise, it knows that the device is not authenticated. Algorithm 3 and Figure 3 show the steps that the blockchain performs to ensure party authentication.

Algorithm 3 Party-authentication algorithm

```
Checkparties(AD( $P_i$), AD($D_i$))
Input: AD( $P_i$), AD($D_i$)
Output: True or false
Begin
    $B_s$ combines $AD(D_i)$ with $AD(P_i)$ and stores it in message variable
    HashM=SHA-256(message, "hello")
    $P_i$combines $AD(D_i)$ with $AD(P_i)$ and stores it in message variable
    Hashp=SHA-256(message, "hello")
    $P_i$ sends Hashp to $M_i$
    $D_i$combines $AD(D_i)$ with $AD(P_i)$ and stores it in message variable
    HashD= SHA-256(message, "hello")
    $D_i$ sends HashD to $B_s$
    $B_s$ compares between (HashM and Hashp and (HashM and HashD)
    $If$ they eqaul
        return true
    End
    Return false
End
```

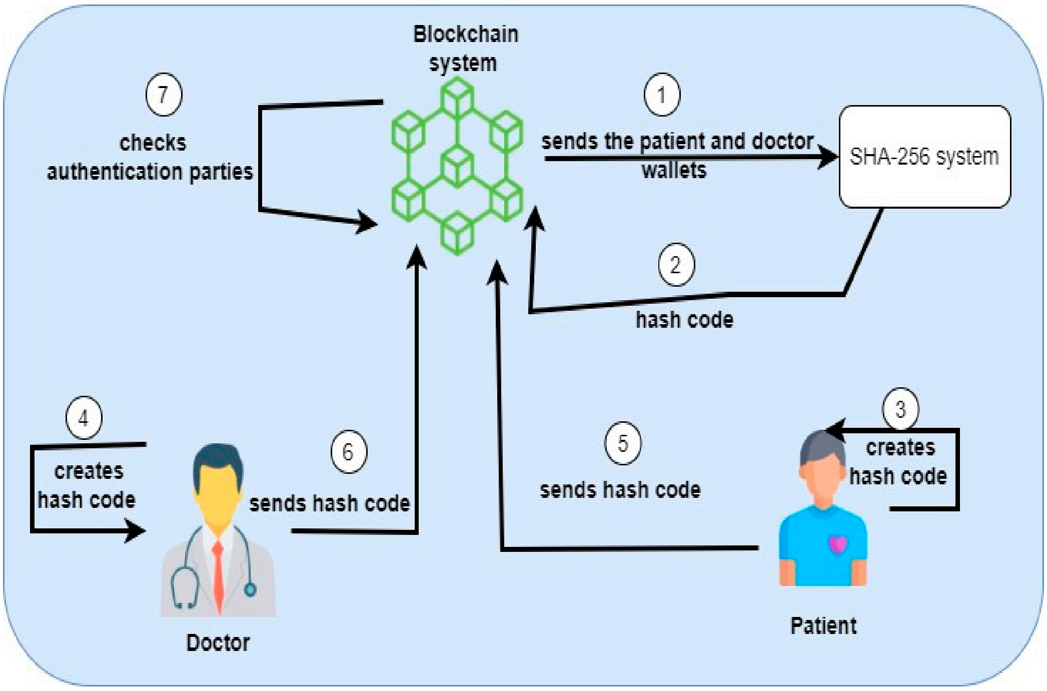

Figure 3. Party-authentication technique.

4. Experiments and Result

In the blockchain, each wallet has an address. We suppose that we have three wallets in our blockchain. Table 3 shows the three wallets that we have in our blockchain.

Table 3. Patients' and doctor's wallets.

Address	Person
142578561452236	Patient 1
47852134478562	Doctor 1
1478523614585	Patient 2

The IoT system that we developed before collects the vital signs of patient 1 and sends them to the blockchain, which then creates a new block. Table 4 shows the information that the blockchain stores in the block.

Table 4. Blockchain data.

Address	Person	Vital Signs	Doctor Address
142578561452236	Patient 1	Temperature = 29 degrees Blood pressure = 90/60 Heart rate = 70 beats per minute	47852134478562

The blockchain uses the previous information and the last block hash code to create a new hash using a modified SHA-256 algorithm. Table 5 shows the hash code that results from the previous transaction.

Table 5. Block 1 hash function.

Block Number	Hash Code
1	affj4568fffe1425368asdff45fr1235fad486d5c2s3f64f58fc6f8fff52ff

Table 5 shows that we do not permit the hash code to start with zeros. Therefore, the system must trust the two parties (patient and doctor). The blockchain uses the party-authentication technique to do this. Table 6 shows how the blockchain authenticates parties.

Table 6. Party-authentication example.

Steps	Example
Patient wallet address	142578561452236
Doctor address	47852134478562
Combine the two addresses together	4785213447856214 2578561452236
Combine them with the word hello	47852134478562142578561452236hello
Use modified SHA-256 to hash message	85df30a94d1127d9a6e2a3b58471a45729 ece04a0b59a497ab18efdf4a7b796

Table 6 shows that the blockchain combines the patient's wallet address with the wallet address of the doctor and adds the hello word to them. Then, the blockchain uses SHA-256 to hash the message that results from the combination. The patient's and doctor's devices perform the same previous steps to obtain the hash. Then, they send that hash to the blockchain, which compares it with the calculated hash code. If the two hash codes are not equal, the blockchain stops the operation. Otherwise, the blockchain creates a new contract between patient 1 and doctor 1, and the physician can access the blockchain to see the vital signs of the patient. After the doctor receives the vital signs, they respond with the treatment that the patient must take. Table 7 shows the treatment that the doctor sends to the patient.

Table 7. Doctor response.

Address	Person	Treatment	Doctor Address
47852134478562	doctor 1	You will be in a good state if you take one aspirin.	142578561452236

The blockchain creates a new block to store the doctor's response. The new block will create a hash code for that block by using the doctor's response and the hashing of the last block. Table 8 shows the hash code that represents the new block.

Table 8. Block 2 hash function.

Block Number	Hash Code
2	f78fd4c7g8h5df75c1b2f442535f74fc45f4sf4b4s5safff55fff74fc87f58

Finally, the blockchain permits the patient to see the treatment that the doctor sent to the patient. Table 9 shows the blockchain blocks after the process is ended.

Table 9. Blockchain blocks.

Last Hash	Stamp Time	Address (Sender)	Address (Receiver)	Data	Hash	Nonce
0	4785123021456				f84s5c1g45768r4f4s5dfet8fh4nfb2fgff8f4fb5f2fadc4efaf568456dfef	0
F84S5C1G45768R4F4S5DFET8FH4NFB2FGFF8F4FB5F2FADC4EFAF568456DFEF	1478412367445	14257856145 2236	47852134478562	Temperature = 29 degrees Blood pressure = 90/60 Heart rate = 70 beats per minute	affj4568fffe1425368asdff45fr1235fad486d5c2s3f64f58fc6f8fff52ff	15
AFFJ4568FFFE1425368ASDFF45FR1235FAD486D5C2S3F64F58FC6F8FFF52FF	1478523645123	47852134478 562	142578561452 236	You will be in a good state if you take one aspirin.	f78fd4c7g8h5df75c1b2f442535f74fc45f4sf4b4s5safff55fff74fc87f58	832

The robustness of blockchain is measured by four attributes [31]. The four characteristics of blockchain robustness are the hashing code cannot be reversed, blocks must be linked together, a consensus algorithm exists, and the blockchains are decentralized. We showed that our proposed method used a modified SHA-256 hash function algorithm. This function produces a hash code that cannot be reversed. We also proved that the hash function hashed the transaction information and previous block hash code together, so our blockchain linked the blocks together. The proposed system used an Ethereum blockchain platform that used Proof of Stake as a default consensus algorithm. Finally, the proposed blockchain used a distributed ledger, which means that it is decentralized. Therefore, this proposed blockchain method is more robust. The proposed method used a party-authentication technique that checks the individuals' identities before they can access the data. We also show that it is very difficult to change any block information. This means that the proposed method is dependable.

We adjusted the hashing function by compressing data with the LZ4 algorithm. As a result, assuming the hashing code does not begin with multiple zeros, the time complexity of our proposed method is O(n), where n is the size of the hash function. The time is decreased by using LZ4 data compression. Because building a smart contract does not require much time, the time complexity for doing so is O(1).

Table 10 presents the comparisons between some related work, blockchain versions, and our proposed method. Table 10 further demonstrates that the proposed method takes one second to create a new block while all blockchain versions take longer than that. This table also shows that the proposed technique is expandable because a decentralized database is utilized. From Table 10, it is seen that our proposed system's time complexity is lower than that of all current approaches. The time complexity of blockchain 3.0 is equal to the time required by our previous proposed method. However, because the proposed technique employs LZ4 to compress data, it requires less time than blockchain 3.0 or our previous method takes. The time required to construct a certain number of blocks using all current techniques and our suggested methodology is depicted in the following figure. Figure 4 demonstrates how our proposed approach may build several blocks in 1 min. If we want to create 500 transactions, we must be able to build 500 transactions. Building 500 blocks will take 500 s or 8.5 min using our proposed method. Blockchain 1.0 will construct the 500 blocks in 90,000 s, or 25 h. Building the same number of blocks will take 7000 s (2 h) on blockchain 2.0. The 500 blocks on blockchain 3.0 will be constructed in 1000 s or 17 min. Our pervious blockchain system takes 750 s (12.5 min) to build 500 blocks. Table 10 proves that our proposed approach performs better because it takes slightly longer to generate the block than other methods since it employs the LZ4 algorithm to compress the data. Figure 4 again demonstrates how quickly any number of blocks may be constructed using our proposed technique. Table 10 also shows that our system ensures the identification of the patient and the doctor using a party-authentication technique. Figures 4 and 5 show the results of new experiments using the same experimental settings to compare these methods with the proposed system.

Table 10. Comparison between related work and proposed method.

Measurements	BLOCKCHAIN 1.0	BLOCKCHAIN 2.0	BLOCKCHAIN 3.0	BAIJU [22]	IBRAR [20]	Asma Khatoon [21]	Our Previous Aork [22]	Proposed System
Data that secure	Cryptocurrency	financial	financial	Medical data	Medical data	Medical data	Medical data	Medical data
Scalability	✗	✗	✗	✗	✗	✗	✓	✓
Interoperability	✗	✗	✓	✗	✗	✗	✓	✓
Address can be read	✗	✓	✗	✓	✓	✓	✓	✓
Transaction time	2–4 (min)	14 (s)	14 (s)	14 (s)	14 (s)	14 (s)	1–2 (s)	1.5 (s)
Time complexity	O(n^2)	$n \log n$	O(n + d)	$n \log n$	$n \log n$	$n \log n$	O(n + d)	O(n)
Party authentication	✗	✗	✗	✗	✗	✗	✗	✓

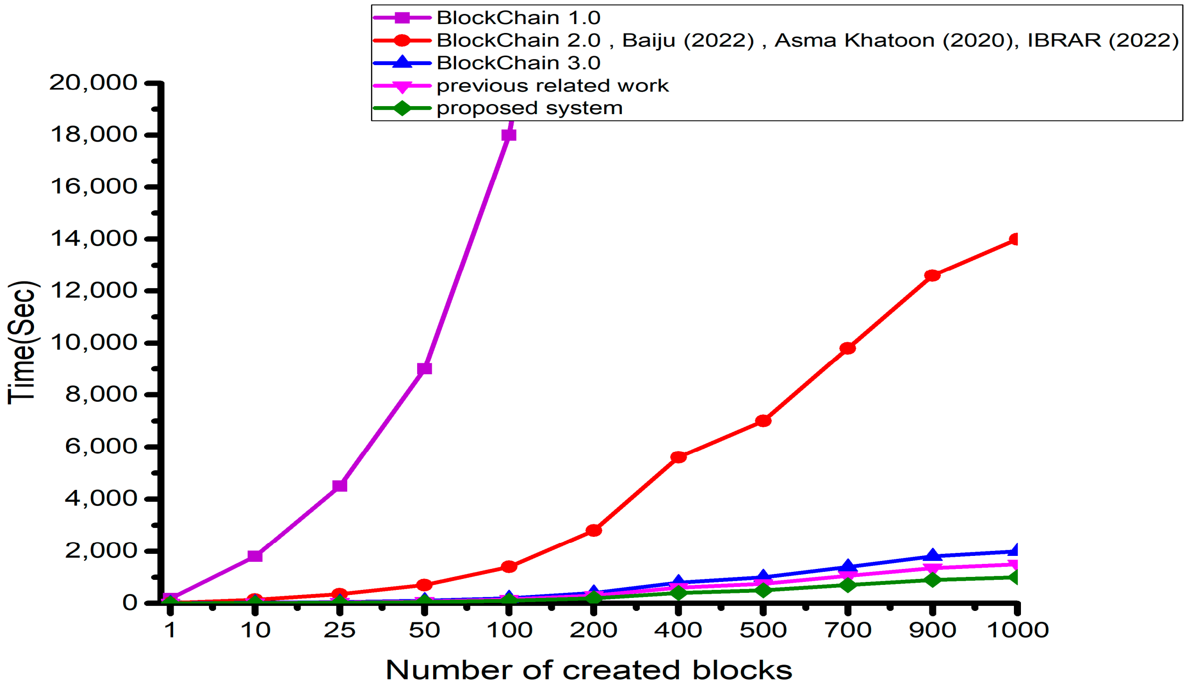

Figure 4. Comparison between all related work and proposed method.

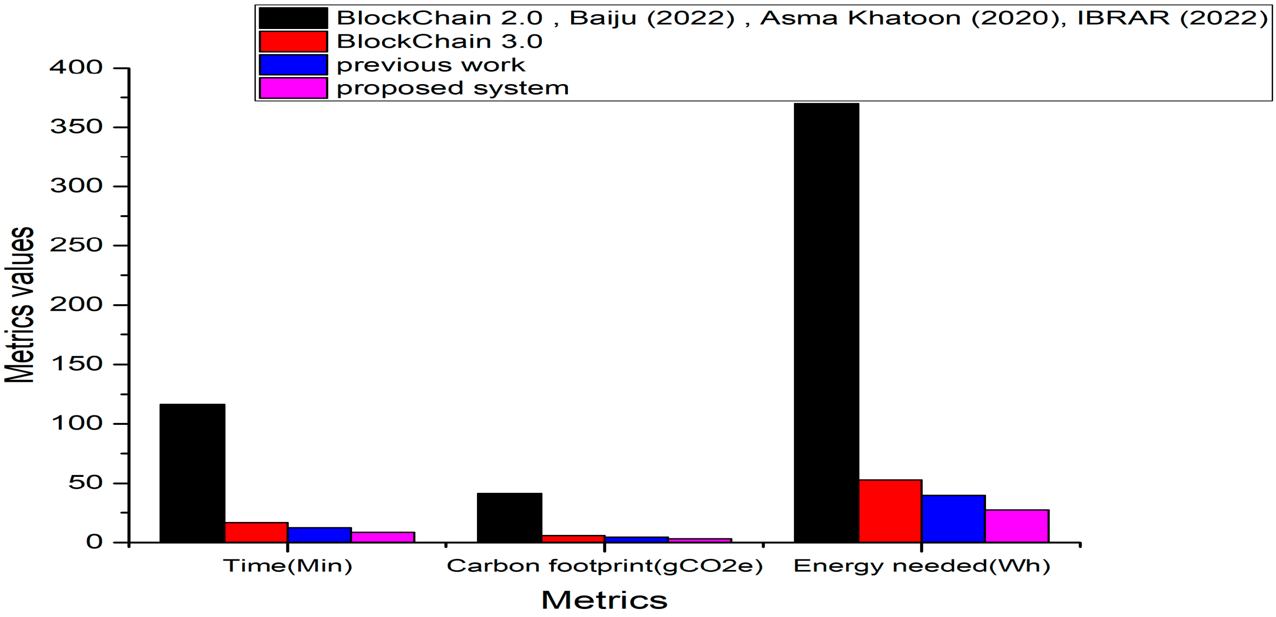

Figure 5. Green computing analysis.

We also analyze our system and other blockchain versions according to green computing rules. Figure 5 shows the analysis of our system and related works when there is a need to create 500 blocks. We exclude blockchain 1.0 because it gives the worst results. This result happens because it takes 25 h to create 500 blocks. Figure 5 shows that we use three metrics to compare the proposed method and blockchain versions: the time to create 500 blocks, carbon footprint, and energy needed. A carbon footprint measures the entire amount of greenhouse gases produced by our daily activities. Energy needed metrics show the electricity needed to create 500 blocks. Figure 5 shows that our proposed system does not require a large quantity of energy to create 500 blocks. It takes 27.25 WH. Figure 5 also shows that the carbon footprint needed is 3.03 g Carbon dioxide equivalent (CO2e). Figure 5 also shows that our previous system performs better than all other blockchain versions. It needs 39.61 WH energy to create 500 blocks. Blockchain 3.0 performs better than blockchain 2.0. It consumes 52.91 WH energy, while blockchain 2.0 consumes 369.77 WH.

5. Conclusions

Because blockchain is decentralized, it is difficult to hack. The hacker must alter all the ledgers to access the data held in any block. As a result, data extraction from a blockchain is very difficult if it contains several blocks. To stop hackers from stealing or changing the data, we present a novel method to safeguard patient data utilizing blockchain in this study. In this paper, we use blockchain to create a management system to store medical data. This system stores the vital signs as a block in the blockchain and then stores the treatment as a new block in the blockchain. We use a modified version of SHA-256. This modified version uses LZ4 to compress data. Thus, our suggested medical blockchain creates a block in O(n), where n is the size of the hash function. In future work, we intend to use artificial intelligence techniques to replace the doctor with automatic tools to be able to send the treatment to the patient without waiting for a doctor's response. We also intend to decrease the number of blocks by storing the information between the same doctor and the same patient in the same block.

Author Contributions: Conceptualization, I.S.F., M.E., S.E. and A.E.T.; methodology, I.S.F., W.A., M.E., S.E. and A.E.T.; software, I.S.F.; validation, W.A., M.E., S.E. and A.E.T.; formal analysis, I.S.F. and A.E.T.; investigation, W.A., M.E. and S.E.; writing—original draft preparation, I.S.F., W.A., M.E., S.E. and A.E.T.; writing—review and editing, I.S.F., W.A., M.E., S.E. and A.E.T.; visualization, I.S.F.,

W.A., M.E., S.E. and A.E.T.; supervision, W.A., M.E., S.E. and A.E.T. All authors have read and agreed to the published version of the manuscript.

Funding: There is no external fund for that research.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that there are no conflict of interest.

References

1. Lopes, A.R.; Dias, A.S.; Sá-Moura, B. Application of technology in healthcare: Tackling COVID-19 challenge–the integration of blockchain and Internet of Things. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; IGI Global: Hershey, PA, USA, 2023; pp. 108–131.
2. Salamai, A.A. An approach based on decision-making algorithms for QoS-aware IoT services composition. *JISIoT* **2023**, *8*, 8–16. [CrossRef]
3. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.-V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.-M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inf. Decis. Mak.* **2020**, *20*, 1–10. [CrossRef] [PubMed]
4. Alhadhrami, Z.; Alghfeli, S.; Alghfeli, M.; Abedlla, J.A.; Shuaib, K. Introducing blockchains for healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Aurak, United Arab Emirates, 21–23 November 2017; pp. 1–4.
5. Roe, D. Top 5 Internet of Things Security Concerns. Available online: https://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php (accessed on 11 November 2022).
6. Thota, C.; Sundarasekar, R.; Manogaran, G.; Varatharajan, R.; Priyan, M.K. Centralized fog computing security platform for IoT and cloud in healthcare system. In *Fog Computing: Breakthroughs in Research and Practice*; IGI Global: Hershey, PA, USA, 2018; pp. 365–378.
7. Atassi, R.; Al-hosban, F. Fusion optimization and classification model for blockchain assisted healthcare environment. *Fusion Pract. Appl.* **2022**, *9*, 62–73. [CrossRef]
8. Farahat, I.S.; Tolba, A.S.; Elhoseny, M.; Eladrosy, W. A secure real-time internet of medical smart things (IOMST). *Comput. Electr. Eng.* **2018**, *72*, 455–467. [CrossRef]
9. Tanriverdi, M. A systematic review of privacy preserving healthcare data sharing on blockchain. *J. Cybersecur. Inf. Manag.* **2020**, *424*, 31–37. [CrossRef]
10. Kazia, E. Blockchain-based model for image encryption in IoT communication environment. *Int. J. Wirel. Ad Hoc Commun.* **2022**, *5*, 54–64. [CrossRef]
11. Kamruzzaman, M.M.; Yan, B.; Sarker, M.N.I.; Alruwaili, O.; Wu, M.; Alrashdi, I. Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities. *J. Healthc. Eng.* **2022**, *2022*, 9957888. [CrossRef]
12. Deepa, N.; Pham, Q.-V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Gener. Comput. Syst.* **2022**, *131*, 209–226. [CrossRef]
13. Choi, T.-M.; Siqin, T. Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transp. Res. Part E Logist. Trans. Rev.* **2022**, *160*, 102653. [CrossRef]
14. Aggarwal, S.; Kumar, N. Blockchain 2.0: Smart contracts. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 301–322.
15. Maesa, D.D.F.; Mori, P. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* **2020**, *138*, 99–114. [CrossRef]
16. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *J. Food Qual.* **2021**, *2021*, 7608296. [CrossRef]
17. Macdonald, M.; Liu-Thorrold, L.; Julien, R. The blockchain: A comparison of platforms and their uses beyond bitcoin. *Work Pap.* **2017**, *1*, 1–18.
18. Yu, H.; Sun, H.; Wu, D.; Kuo, T.-T. Comparison of smart contract blockchains for healthcare applications. *AMIA Ann. Symp. Proc.* **2019**, *2019*, 1266.
19. Chowdhury, M.J.M.; Ferdous, M.D.S.; Biswas, K.; Chowdhury, N.; Kayes, A.S.M.; Alazab, M.; Watters, P. A comparative analysis of distributed ledger technology platforms. *IEEE Access* **2019**, *7*, 167930–167943. [CrossRef]
20. Rupa, C.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. A blockchain based cloud integrated IoT architecture using a hybrid design. *Int. Conf. Collab. Comput. Netw. Appl. Worksharing* **2021**, *350*, 550–559.
21. Bigini, G.; Freschi, V.; Lattanzi, E. A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. *Future Internet* **2020**, *12*, 208. [CrossRef]
22. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
23. Li, P.; Nelson, S.D.; Malin, B.A.; Chen, Y. DMMS: A decentralized blockchain ledger for the management of medication histories. *Blockchain Healthc. Today* **2019**, *2*, 38.

24. Ktari, J.; Frikha, T.; ben Amor, N.; Louraidh, L.; Elmannai, H.; Hamdi, M. IoMT-based platform for E-health monitoring based on the blockchain. *Electronics* **2022**, *11*, 2314. [CrossRef]
25. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
26. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [CrossRef]
27. Baiju, B.V.; Saranya, S.; Sriram, D.; Ahmed, M.R.; Mohammed, A. Decentralizing Electronic Medical Records on the Blockchain Using Smart Contracts. *J. Pharm. Negat. Results* **2022**, *13*, 311–316.
28. Mehbodniya, A.; Webber, J.L.; Neware, R.; Arslan, F.; Pamba, R.V.; Shabaz, M. Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data. *Expert Syst.* **2022**, *39*, e12978. [CrossRef]
29. Farahat, I.S.; Aladrousy, W.; Elhoseny, M.; Elmougy, S.; Tolba, A.E. Improving Healthcare Applications Security Using Blockchain. *Electronics* **2022**, *11*, 3786. [CrossRef]
30. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.K.M.N.; Shorfuzzaman, M. Permissioned blockchain and deep-learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Trans. Ind. Inf.* **2022**, *18*, 8065–8073. [CrossRef]
31. Zaher, M.; ElGhitany, N.E.K. Blockchain communication platform selection in IoT healthcare industry using MARCOS. *Int. J. Wirel. Ad Hoc Commun.* **2021**, *2*, 49–57. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.