electronics

MDPI

Article

Improving Healthcare Applications Security Using Blockchain

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

[1] Faculty of Computers and Information, Luxor University, Luxor 85951, Egypt
[2] Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[3] College of Computing and Informatics, University of Sharjah, Sharjah 27272, United Arab Emirates
[*] Correspondence: ishawky@fci.luxor.edu.eg

Abstract: Nowadays, the Internet of Medical Things (IoMT) technology is growing and leading the revolution in the global healthcare field. Exchanged information through IoMT permits attackers to hack or modify the patient's data. Hence, it is of critical importance to ensure the security and privacy of this information. The standard privacy techniques are not secured enough, so this paper introduces blockchain technology that is used for securing data. Blockchain is used with the smart contract to secure private patient records. This paper presents how a patient may send his vital signs to the physician through the Internet without meeting with the latter in person. These vital signs are collected from the IoMT system that we developed before. In the proposed method, each medical record is stored in the block and connected to the previous block by a hashing function. In order to secure the new block, the SHA256 algorithm is used. We modified the SHA256 algorithm by using run-length code in compressing data. If any hacker attempts to attack any medical record, he must change all previous blocks. In order to preserve the rights of the doctor and patient, a smart contract is built into the blockchain system. When the transaction begins, the smart contract withdraws the money from the patient's wallet and stores it in the smart contract. When the physician sends the treatment to the patient, the smart contract transfers the money to the physician. This paper shows that all recent work implements Blockchain 2 into the security system. This paper also shows that our security system can create a new block with O (n + d) time complexity. As a result, our system can create one hundred blocks in two minutes. Additionally, our system can deposit the money from the patient's wallet into the physician's wallet promptly. This paper also shows that our method performs better than all subsequent versions of the original blockchain.

Keywords: Internet of Things; Internet of Medical Things; blockchain; medical smart contract; security

check for updates

Citation: Farahat, I.S.; Aladrousy, W.; Elhoseny, M.; Elmougy, S.; Tolba, A.E. Improving Healthcare Applications Security Using Blockchain. *Electronics* **2022**, *11*, 3786. https://doi.org/10.3390/electronics11223786

Academic Editor: Esteban Tlelo-Cuautle

Received: 25 October 2022
Accepted: 15 November 2022
Published: 17 November 2022

1. Introduction

The phenomenon of medical data is expanding more rapidly than ever. Every second, new data are created at a rate of almost 1.7 megabytes. These records must continue to be protected since they include sensitive personal data [1]. A public tracking website for data breaches, Breach Level Index, says that since 2013, almost 9,198,580,293 data records have been lost or stolen [2]. Over the past ten years, the amount of data has increased rapidly, but shoddy security procedures still put firms in danger of a data breach. Personal medical information is one of the main issues regarding data privacy. Additionally, computers today are full of vulnerabilities that hackers use to steal any data on them. According to a graph published by the National Institute of Standards and Technology (NIST), 18,378 vulnerabilities were discovered in 2021 [3]. Table 1 depicts the NIST statistics of the number of vulnerabilities that are discovered each year. Table 1 also shows that the number of vulnerabilities increases every year. In recent years, many systems have been developed to protect and secure personal medical data. Some of the related works suggest storing medical data in centralized storage. This idea provides a better way to protect the data, but two problems ensue. The first problem is having the space that permits storing a massive amount of sensitive data. The other problem is how to secure data despite unauthorized access. Therefore, the other related works use decentralized storage to store the data. Additionally, they suggest that the blockchain is the best tool for storing that data because the hacker must change all the ledgers in order to hack it. Therefore, using many blocks to store data makes it very difficult to be hacked. Additionally, hashing the new block with the transaction information and starting the hash with the fixed number of zero adds additional difficulty to obtaining any information. Any change of one block without changing all the previous blocks will be easily caught by the blockchain, so the data are secured.

Table 1. NIST graph according to [3].

Year	Number of Vulnerabilities
2015	9867
2016	11,207
2017	16,585
2018	17,814
2019	17,416
2020	18,335
2021	18,378

This paper focuses on implementing a system that helps patients obtain their treatment without going to a physician in person. They have to use the Internet to send their vital signs. Following this, the physician sends the treatment to the patient through the Internet. This paper focuses on implementing a security system that protects medical data from being stolen or hacked by anyone. This paper also guarantees the transaction of the money from the patient's wallet into the physician's wallet after the physician sends the treatment to the patient.

This paper aims to contribute to the scientific field by proposing:

- A blockchain security system that secures the medical data collected from the Internet of Medical Things (IoMT) system that we designed and implemented before [4];
- A blockchain security system that uses SHA-256 to hash the new block. We modified SHA-256 by using a run-length code algorithm to compress data;
- A new smart contract technique that guarantees the transaction of the money from the patient's wallet into the physician's wallet after the physician sends the treatment to the patient.

The proposed system consists of two main parts. The first part creates a new block for each transaction using the information of the last block in the blockchain. The second part builds a smart contract between the physician and the patient to guarantee a successful transaction by automatically withdrawing the money from the patient's wallet and transferring it into the physician's wallet.

This paper is organized as follows: In Section 2, the background of the blockchain and some related works are presented. The mathematical model of the blockchain and the proposed method are introduced in Section 3. The results and discussion are presented in Section 4. Finally, the conclusion is explained in Section 5.

2. Background

Computer science and information technology have moved toward a new technology called the Internet of Things (IoT). The IoT field connects all objects surrounding us with each other using computing terms such as sensors, microcontrollers, transmitters, and receivers [5]. The IoT has a lot of applications in many civil and military fields such as smart homes, smart cities, agriculture, and healthcare systems. Nowadays, the IoT has moved toward improving individual health. It is still in the first steps of advancement in the field of healthcare systems [6,7] under the denomination Internet of Medical Things (IoMT).

The IoMT is maintained by connecting some of the medical sensors with microcontrollers. Now, it tries to connect all stakeholders of healthcare systems, such as physicians, patients, and hospital staff, despite their different locations. On the IoMT, data travel across the network to be sent from patient to physician to become easy for physicians to monitor their patients. However, hackers can attack these data over the network and can thus modify or steal them. Hence, securing these data is a big challenge faced by the IoMT. Table 2 shows the security problem that the IoMT and the IoT face according to David Roe's report [8].

Table 2. Security problems faced by the IoMT and IoT [8].

Security Problem	Percentage
Insufficient authentication	80%
Unencrypted communication	70%
Privacy concerns	90%

Blockchain [9–12] is a roster of ledgers which are called blocks. Each block is connected to the previous block using a cryptographic hash function [9,13]. Each block contains information about the timestamp, data, and previous block hashing [13], so these blocks look like a tree with a hash tree root. The blockchain is a distributed database which executes transactions between both ends of the connection efficaciously, in a demonstrable and permanent way [14]. It appears as peer-to-peer network which has a protocol for inter-node communication and verifying newly created blocks. When a block is created, no one can change any block information without the alteration of all the sequential blocks. In 2008, Satoshi Nakamoto was the first person to create the cryptocurrency Bitcoin with a public transaction ledger; he then developed the public ledger to the distributed ledger and called it blockchain [14]. Blockchain helps Bitcoin to solve the problems of ordinary money such as double-spending problems and the problem of needing a central server or third party authority such as the bank [15].

Today, blockchain is used in every field of computer science, especially in encryption, privacy, finance, healthcare, and economics. Blockchain can be used in healthcare; for example, it can be applied to electronic health records, drug traceability from industrialist to clients, clinical tests to rub fraudulent data adjustment, interoperability, etc. [14,16]. In 1993, Nick Szabo invented a new concept called a smart contract. Now, the smart contract is implemented in the blockchain used by the Ethereum coin. The idea of Nick Szabo was to introduce the protocol for the computerized deals which appears as a contract [17]. He converted transaction clauses such as collateral into code by converting transactions into the concept of software and hardware, which can be achieved easily. After Szabo implemented the smart contract, he showed that the smart contract avoids the need of intermediaries which appear between transacting parties, such as the bank [18]. Smart contracts are scripts saved on the blockchain. They can appear as stored functions in the database management system [19]. The smart contract has some properties such as autonomy, trust, backup, savings, and accuracy. It can be used for the exchange of money, ownership, or anything that needs to be transparent without needing a middleman. It defines the principles and retribution of the transaction as the traditional contract does and also automatically ensures those commitments are maintained. When parties execute transactions between each other, this transaction is stored on blockchain as more than a simple record. This blockchain permits programs to be executed and stores the transaction as ledger: this is called smart contract. These programs are not smart and not used for the execution or monitoring of contracts.

Solidity is a high-level language in which syntax looks like Javascript. The Solidity language was created to execute smart contract code for the Ethereum virtual machine. Some examples of Solidity coding are voting, simple open auction, electronic currency, currency, safe remote purchase, and micropayment channel. The smart contract starts to appear with Blockchain 3. Before Blockchain 3, blockchain had the simple form of the smart contract.

Satoshi Nakamoto [20] built the blockchain for financial transactions, but there is a new form of blockchain that works as a distributed database because it stores data about the transaction. These data are an official Bitcoin structure since 2014 [20–23] that can support 80 bytes of data. Scientists started to increase the data size. For example, with Multichain [22], which increases the amount of data per transaction, and BigchainDB [23], which uses RethinkDB [24] as a database so there is no limitation in data size. Scientists started to use blockchain to spread slightly drilled sites online using machine learning frameworks between participating sites. This version of blockchain is called Blockchain 2.0. Blockchain 2.0 records the properties of the blockchain and smart contract [25–28]. The most famous application of Blockchain 2 is Ethereum [29,30], which is the decentralized database using a smart contract. Ethereum had been built using a Turing programming language that supports loop calculation, which does not exist in Bitcoin's scripting language. Nowadays, a new version of blockchain called Blockchain 3.0, has been proposed to indicate applications beyond the economy, markets, and currency [31].

In Blockchain 3.0, researchers are trying to adapt the blockchain to work with healthcare applications. For example, Irving et al. [32] used blockchain as a distributed ledger to proof tamper and provide a proof to specified endpoints in the clinical trial. McKernan [33] proposed a system that uses a decentralized blockchain to store genomic data. Jenkins et al. [34] discussed how to increase data security using blockchain. There are some applications that are developed to store electronic health records using blockchain [35,36] and record health transactions [37]. Tsung-Kuo et al. [38] were the first to develop the system using blockchain to improve the security and privacy of healthcare data. They built a new model called model chain that adapts the blockchain technology with privacy-preserving machine learning and design a new algorithm to secure the new proof of information by blockchain.

There is significant recent research that starts to implement blockchain with the smart contract, for example, in [39], the authors developed MedRec as a solution to collect the information about medical researchers, patients, and the treatment community. The system was built using blockchain and the smart contract to create a decentralized ledger to store health data. Clinical experiments of the scientific truthfulness of the results can be exposed to some problems such as missing data, selective publication, and endpoint switching. This problem had motivated by Nugent et al. [40] to develop a method using blockchain with smart contracts to record endpoints in clinical experiments. In 2016, International Business Machines (IBMs) invented a system which uses blockchain to protect information from devices, such as the barcode-scanned events, which send data to blockchain ledgers to update and validate the smart contracts [41]. Smith [42] used blockchain and the smart contract to present a way to execute data transactions and change the data to make it easier to add them to the supply chain. Savelyevin [43] discussed the difference between smart contract and contract law and discussed the key properties and features of the smart contract.

Shuai et al. [44] proposed a methodical and thorough analysis of blockchain-enabled smart contracts. The authors presented a framework for smart contracts based on a revolutionary six-layer architecture. The authors also outlined the basic platforms and workings of blockchain-enabled smart contracts. The authors provided a number of common application scenarios. This paper aims to serve as a useful resource and guide for future research projects.

Adam et al. [45] examined the recently published literature on decentralized governance systems and incorporated the insights it articulates on blockchain technology and smart contracts. The authors used a Shiny app to contain evidence-based obtained and handled data. They incorporated the key findings and strong connections connected to smart urban governments by analyzing the most recent and pertinent sources and utilizing screening and quality evaluation methods including AMSTAR, Dedoose, Distiller SR, ROBIS, and SRDR. The dimensions were used as data visualization tools for the original bibliometric mapping, together with the VOSviewer layout techniques.

Researchers have started using blockchain in medical fields, such as Kristen et al. [46] who suggested using blockchain-based smart contracts to enable the safe analysis and administration of medical sensors in order to handle the protected health information (PHI) produced by these devices. The authors developed a system wherein the sensors interact with a smart device that collects smart contracts and logs all occurrences on a private blockchain based on the Ethereum protocol. Sending notifications to patients and medical experts, while also keeping a secure record of who initiated these actions, may enable real-time patient monitoring and medical treatments. This will automate the distribution of notifications to all interested parties in a HIPAA compliant way and address various security flaws related to remote patient monitoring. Additionally, Ashutosh et al. [47] present the idea of blockchain and smart contracts and how they may be used in the Internet of Medical Things (IoMT) in the field of electronic healthcare. In addition to outlining a unique architecture, this paper analyzes the directions in which decentralization and the usage of smart contracts will take the IoMT in e-healthcare as well as the benefits, difficulties, and upcoming trends associated with their combination. When compared to conventional methods, the suggested architecture exhibits superior performance in terms of average packet delivery ratio, average latency, and average energy efficiency.

Khatoon [48] examined current research and blockchain-based applications for the healthcare sector. Additionally, for better data management, she suggests several processes for the healthcare sector utilizing blockchain technology. The Ethereum blockchain platform has been used to develop and implement a variety of medical processes, including complicated surgical and clinical trial procedures. Accessing and controlling a sizable amount of medical data are also included. The cost of implementing the medical smart contract system's workflows for managing healthcare has been evaluated in terms of a feasibility study, and this paper's thorough presentation of that study has provided a cost estimate for said system. This paper will make it easier for many medical system participants to provide better healthcare services while reducing costs.

Baiju et al. [49] used a blockchain design built on the Ethereum blockchain. Their system uses truffle as a building block. With the aid of the consensus calculation, smart contracts are used to manage the availability of the EMRs. The contracts are used inside the system to monitor the transactions and calculations involved in the management of customer information. Since medical information is quite different from cryptocurrencies and NFTs, which are resources that have been used with blockchain, we must fundamentally alter our methods to make it feasible. Their system keeps the data using the Dapp wallet address and accessing them and making changes to the patient's information is necessary. When the data is input, it is tunneled over the API to an operational logistic regression model, which analyses the data supplied via the API to ascertain the patient's health status and returns the data after the model has been calculated.

3. The Proposed Secure Medical Blockchain Model

The implementation of our work consists of two parts. The first part introduces the implementation of the blockchain. The second part introduces the implementation of the smart contract. Figure 1 shows the framework of the proposed system.

Figure 1 shows that the proposed system's framework consists of two main parts. The first part is the implementation of the blockchain to secure the data. The second part is the implementation of a smart contract to transfer the money from the patient's wallet into the physician's wallets without using a bank or any middleware.

Figure 1 also shows the patient wanting to ask the doctor about treatment for his status. Then, the proposed system creates a new block using the last block. Therefore, the system creates a new smart contract between physician and patient by obtaining the patient's vital signs from the IoT healthcare system described in [4]. After that, the doctor examines the patient's vital signs and sends the treatment to that patient through the smart contract. Finally, the smart contract automatically sends the money from the patient's wallet into the physician's wallet. The implementation of blockchain medical records must consist of doctors, patients, and records that contain information about each interaction between doctors and patients.

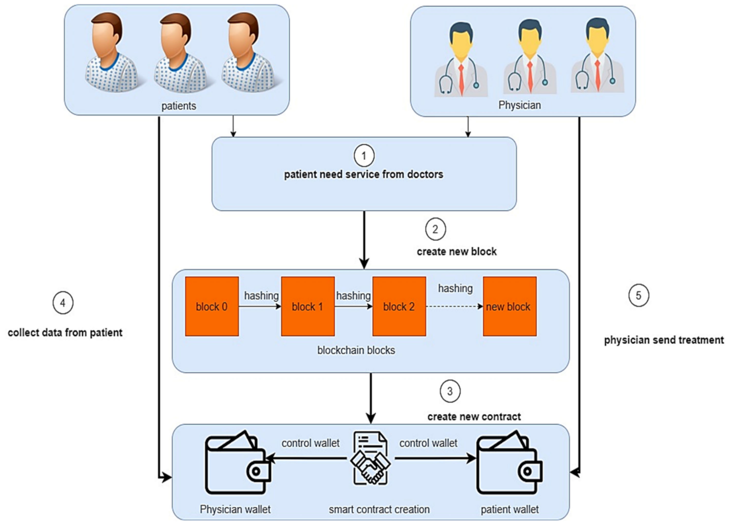

Figure 1. The proposed framework.

For more clarification, Figure 2 shows the application scenario of the proposed system. The previous IoMT that we developed before collects the patients' vital signs. Therefore, the collected data are sent to our microcontroller. The microcontroller sends a request that asks the physician to treat the patient. If the physician agrees, the collected data are sent directly to the blockchain to create a new block. The new block is created using the information of the previous block. After that, the blockchain inserts transaction information into that block and sends data to the smart contract to build a new contract. Then, the smart contract withdraws the money that a physician retrieves after he sends the treatment from the patient's wallet. Therefore, the physician sends the treatment to a smart contract which then sends it directly to the patient. Finally, the smart contract transfers the money into the physician's wallet.

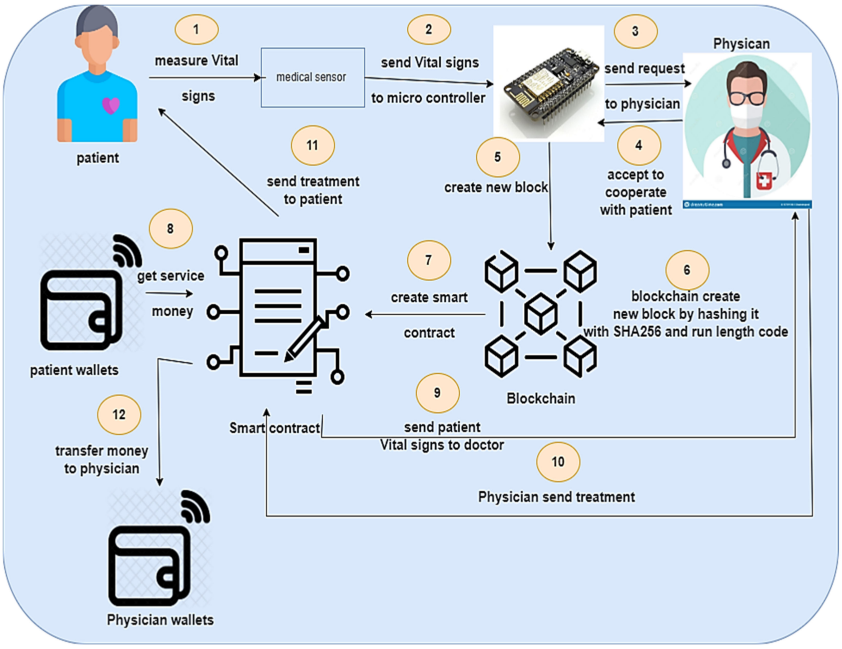

Figure 2. Application scenario of our proposed system.

Figure 3 shows the basic idea of the blockchain.

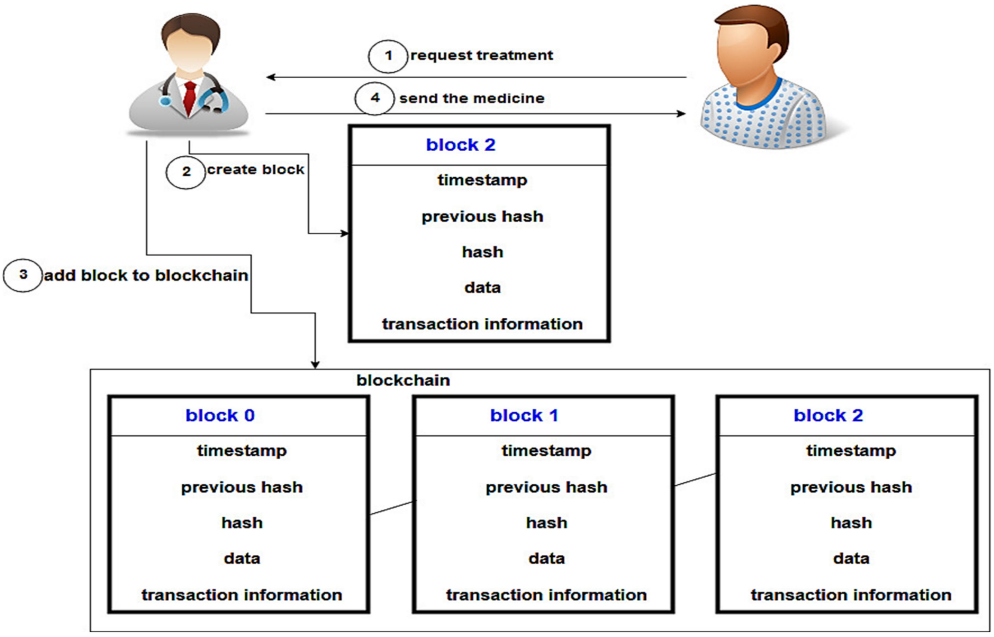

Figure 3. The blockchain-based medical record security system.

Figure 3 shows each patient asking the doctor for treatment. Then, the physician agrees to helping the patient. As a result, the blockchain system starts to create the block with the information about the transaction, the creation time of the block, and the previous and current hash code. The current block is connected to the last block by hashing the information of the current block together with the previous hash code. The new block hashes using the SHA256 algorithm. We also use run-length code to compress the data of the transaction. Then, this block is added to the chain. After that, it is difficult to hack or modify the patient's information because to hack that block, the hacker must extract all the previous blocks.

Since a blockchain is a series of blocks, we must first define a block. A block is the primary piece of data that is kept in a blockchain. The blockchain's function is to store blocks in a secure way. A generic block is indicated by the letters B_r. A block is created when there is a transaction between two entities. Block B consists of many entries with a size N, so a Block can be defined as follows:

$$B_r = (E_1, \ldots, E_N) \tag{1}$$

A mathematical problem called the proof-of-work is used to establish a connection between two blocks. This link will appear in the second block's header. A miner is a person who attempts to identify the proof-of-work. Let us take into consideration two blocks, namely Bp and Bnew, as well as a quantity known as bits and indicated as b. A goal number may be calculated immediately from b, which measures how challenging the proof-of-work is. This target is a 64-digit hexadecimal number that has a significant number of zeros as its leftmost digits, such as:

00fe49cecc0b2f766505fbbafbaa93671f04e680a8b633ff2df529fcbd05b401b8.

The hashing function algorithm that we use in the blockchain is sha-256. We shall define the hash of a particular block shortly after assuming the hash of the preceding block, Hashing (Bp), is known. The equation that we used to calculate the hashing of the new block is as follows:

$$\text{Hashing}(B_{\text{new}}) = \text{Hashing}(\text{Hashing}(B_p\ ) \oplus \text{timestamp}(t) \oplus \text{b} \oplus \text{nonce}) \leq \text{target} \tag{2}$$

where ⊕ denotes the concatenation operation and timestamp(t) denotes the current time.

When the proof-of-work for the blocks Bp and B has been solved, we may specify block B's header using the notations shown above:

$$Header(Bnew) = (i_m,\ Hashing(B_p\ ),\ timestamp(t),\ b,\ nonce,\ Hashing(B_{new})) \quad (3)$$

Algorithm 1 shows the main steps needed to create the blockchain and the content of each block. Table 3 shows the notations that are used in the algorithm.

Table 3. Algorithm notations.

Meaning	Notations
Patient	P_i
Physician	PY_i
System	M
Transaction	T_i
Block	B_i
Blockchain	BS
Hashing	H_i
Original data	O
Asci data	A
Compression function using run-length code	C
Contract before creation	CO_i
Created contract	CC_i
Locked contract	LC_i
Smart contract system	SM
Inactive contract	IC_i

The algorithm transfers the treatment fees into the physician's account. In order to hash a new block in the blockchain, SHA256 is used. The following algorithm shows the algorithm of the SHA256 hashing function that the proposed system used. Algorithm 2 shows that the run-length code algorithm is used to compress data.

Algorithm 1. Private medical blockchain algorithm

```
1: $P_i$ asks $PY_i$ for $T_i$.
2: $T_i$ pends until $M$ creates $B_{new}$; then, $T_i$ is created.
3: $PY_i$ accepts $T_i$ with the $P_i$.
4: $M$ fills $B_{new}$ with the information of the $T_i$.
5: $M$ adds $B_{new}$ to $BS$ by creating $H_i(B_{new})$ depending on the information of $T_i$, such as time of $B_{new}$
   and $H_i(B_{per})$.
6: $M$ checks $BS$ to ensure nothing is changed or missing.
```

The implementation of the smart contract consists of a patient and a physician. The main idea of the proposed system came from the evolution of the healthcare field that guarantees the best care for the patient but does not guarantee that the physician obtains the compensation related to his efforts; therefore, the implementation of a smart contract that serves the healthcare field is critical. The proposed system allows the patient to offer the doctor a certain payment in exchange for treatment, to which the doctor can then agree or disagree. When the doctor agrees to treating the patient, the system creates a new smart contract. Therefore, smart contracts monitor the process of treatments. When the physician sends the treatment to the patient, the money is automatically transferred into the physician's wallet. The money is returned to the patient's wallet if the doctor does not treat the patient.

Algorithm 2. Hashing function of the blockchain algorithm

```
Algorithm Hashing (O)
1: Convert O into A.
2: A is divided into $B_i$ with a size of 512 bit for each B.
3: If $B_i < 512$,
4: do → expand $B_i$ to 512 by adding padding bits.
5:   $B_i$ is divided into smaller $B_i$ with a size of 32 bit for each B.
6: Iteration = 0.
7: While iteration < 64,
8: do → Apply C to each block.
9: Return H.
```

Figure 4 shows that the patient must initiate the contract by asking the physician to treat him and by determining the payment for the treatment. The physician examines the offered payment and gives his opinion about the contract. If the physician agrees to treat the patient, the amount of money that the patient determined is transferred into the smart contract system from the patient's wallet. The smart contract monitors the physician to verify whether the doctor sends the treatment. If the doctor sends the treatment, the smart contract transfers the money into the doctor's wallet. However, if the doctor does not send the treatment, the money is returned back to the patient. Algorithm 3 describes the steps of our implementation.

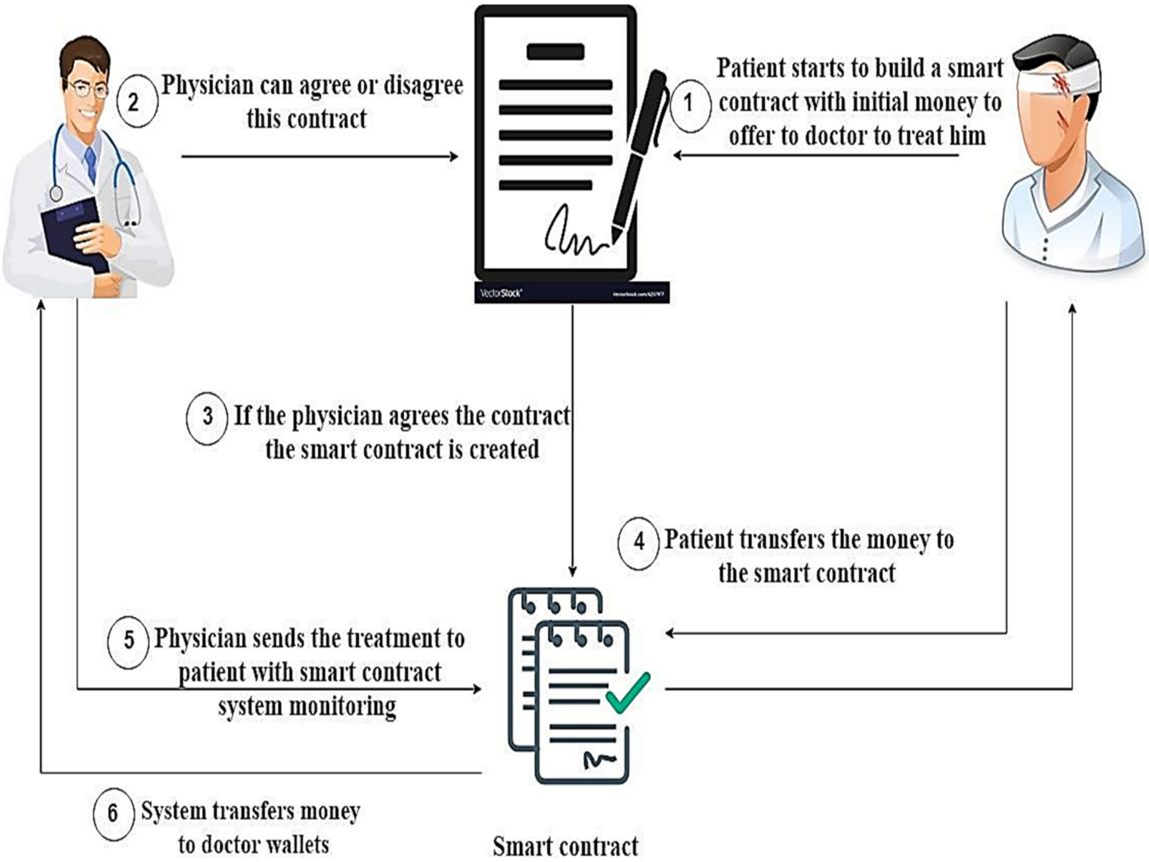
2 Physician can agree or disagree this contract
1 Patient starts to build a smart contract with initial money to offer to doctor to treat him
VectorStock
3 If the physician agrees the contract the smart contract is created
4 Patient transfers the money to the smart contract
5 Physician sends the treatment to patient with smart contract system monitoring
6 System transfers money to doctor wallets
Smart contract

Figure 4. Operations of the smart contract.

In our related work [4], the patient's digital signature is used for authentication before the client delivers vital signs to the receiver. If the authentication succeeds, the system sends the patient's vital signs to the physician.

Algorithm 3. Medical smart contract algorithm

```
1: $P_i$ starts the $CO_I$ with the initial amount of money and offers $PY_i$ to treat him and the statues of $CO_I$ become $CC_i$.
2: If $PY_i$ agrees to $CC_i$, the status of $CC_i$ becomes $LC_i$.
3: The amount of money that $P_i$ determined is transferred to $SM$.
4: $SM$ starts monitoring $PY_i$ to verify whether $PY_i$ sends the treatment to $P_i$.
5: If $PY_i$ sends the treatment to $P_i$, the $SM$ transfers the amount of money of $LC_i$ to $PY_i$ and the status of $LC_i$ becomes $IC_i$.
6: If $PY_i$ does not send the treatment to $PY_i$, the $SM$ returns the amount of money back from $LC_i$ to $P_i$ and the status of $LC_i$ becomes $IC_i$.
```

4. Experimental Results of Blockchain with Smart Contract

Every system user has a wallet and the address and balance of his wallet. Table 4 shows wallets that exist in our system.

Table 4. User wallets before transactions.

User Name	Wallet Address	Balance
Ebrahim	2145867523656	100
Dr Ahmed	154531515656	50
Dr Samir	1548623512586	500

If the patient wants to request any treatment from any physician, he must ask the physician for treatment and transfer money to the physician after treatment. The system verifies the balance of the patient to ensure that the patient has the money that the patient specified; the physician then starts to create a block. Table 5 shows the offer of the patient and the block creation by a physician.

Table 5. The user offers a transaction and the doctor accepts.

User Name	Data Sent	Money Offer	User Received
Ebrahim	25 degrees Celsius	100	Dr Ahmed
Dr Ahmed	Accept transaction	-	Ebrahim

When the physician accepts the transaction, the system creates the block and hashes it by using the information of the transaction and the previous hash. Then, the doctor starts replying to the patient. Table 6 shows the physician's reply to his patient.

Table 6. Physician's reply to patient.

User Name	Data Sent	User Received
Dr Ahmed	You have problem you must take aspirin	Ebrahim

When we verify the balance of the patient and physician, the physician's balance must have increased with the amount specified for the treatment and the patient's balance must decrease by the same amount. Table 7 shows the users' wallets after the transaction.

Table 7. User wallets after transaction.

User Name	Wallet Address	Balance
Ebrahim	2145867523656	0
Dr Ahmed	154531515656	150
Dr Samir	1548623512586	500

Assuming that the amount of treatment fees is 100 pounds, the balance of the physician's wallet is increased by 100 pounds and becomes 150 pounds. This is because the doctor's wallet had 50 pounds before the transaction. Additionally, the balance of the patient's wallet becomes zero because it is decreased by the amount of the transaction. Table 8 shows the status of the blockchain after the previous transaction.

Table 8. Blockchain status.

Previous Hash	Time to Stamp	From Address	From Address Balance	To Address	To Address Balance	Amount of Transaction	Data	Hash	Nonce
0	143228800000							Ff2da8cbc6c99d6846c88baaece037405f1a5779444b651a3a2b9863348	0
FF2DA8CBC6C99D6846C88BAAECE037405F1A5779444B651A3A2B9863348	1531494619742	2145867523656	100	154531515656	50	100	25 degrees Celsius		
		154531515656	50	214586752365	100	0	You have problem you must take aspirin	00fe49cecc0b2f766505fbbafbaa93671f04e680a8b633ff2df529fcbd05b401b8	628

The first block is called genesis block. It does not have any transactions but we use it to create the hash of our second block. This is because the second block creates its hash using the previous hash. Every block contains the transaction from patient to doctor and vice versa. If the doctor does not accept the transaction, the transaction becomes a pending one and neither block nor hash is created. The following Table 9 shows the block state when the doctor does not accept the transaction.

Table 9. Pending transaction.

From Address	From Address Balance	To Address	To Address Balance	Amount of Transaction	Data
2145867523656	100	154531515656	50	100	25 degrees Celsius

The system monitors the blockchain to verify if there is any change in the blockchain, in which case the system replies that there is an error.

In order to guarantee the rights of physician and patient, a smart contract is implemented into the blockchain. We build a method for medical smart contracts and test it using the Solidity programming language in which its compiler is built on the Remix-Ethereum website. The patient starts to deploy the contract and determine the amount of money in it through the value text box. After the patient deploys the contract, the contract in the created state takes a number zero in the code. The first row in Table 10 shows the output of the system when the status of the contract is created.

Table 10. Smart contract states.

Doctor Address	Patient Address	Getter (Money in Patient's Wallet)	State	Value for Transaction
1531494619742	2145867523656	100	0 (create state)	100
1531494619742	2145867523656	100	1 (locked state)	100
1531494619742	2145867523656	100	2 (inactive state)	100
1531494619742	2145867523656	0	2 (inactive state)	100

The first row in the previous table shows the address of the patient's wallet, the address of the doctor's wallet, and the balance of the patient's wallet. Additionally, it shows the state of the contract and the amount of the money in the contract. Now, the doctor can accept or refuse the contract. He accepts the contract by pressing confirm purchase button. If the doctor disagrees, the contract is not created. If the doctor agrees, the contract is created and the status of the contract becomes locked and takes the value one in the code. No one can change this contract now.

After the doctor accepts the contract, the transaction between patient and doctor becomes private by using a hash function between sending data. The following Table 11 shows the hashing message.

Table 11. Hashing message.

Transaction Hash	From Address	To Address
0X20D1D939B55691F554C5CFC9A3F472 25D26F07078F283025497E307EA498A0BA	1531494619742	2145867523656

The smart contract system begins to monitor the transaction between patient and doctor. If the doctor does not send the treatment after some time, the patient can abort the contract by pressing the abort button. Hence, the status of the contract becomes inactive and takes the value 2 in the code. The second row in Table 10 shows the system in an inactive state when the patient aborts the contract.

When the patient aborts the contract, the getter button is 100 units because the money is returned back to the patient due to its balance not changing. However, if the doctor sends the treatment, the smart contract starts to send the data to the doctor's wallet and the patient's balance is decreased. The third row in Table 10 shows the system in an inactive state when the doctor sends the treatment. The fourth row in Table 10 shows that when the physician sends the treatment to the user, the money is transferred from patient to doctor.

In the proposed method, we modified the hashing function by using run-length code to compress data. Therefore, the time complexity of our proposed system is O(n) if the hashing code does not start with some zeros, where n is the size of the hash function. If the hash code for each block starts with a d number of consequence zeros, the time complexity will be O(n + d). By compressing data with run-length code, the time is reduced.

The time complexity for creating a smart contract is O(1) because it does not take much time to build a smart contract.

The following Table 12 shows the comparison between the different versions of the blockchain and some related work with our proposed system.

In the related work, we explain that Blockchain 2 uses Ethereum, as most of the related work. Therefore, the parameter value of Blockchain 2 is similar as it exists in the related work. The only difference is that the related work tries to protect medical data. Table 12 shows that the proposed system takes less than one second to transfer money from a wallet into another. The proposed method is scalable because it uses a decentralized database. Table 12 also shows that transaction time takes from 1 to 2 s, while all versions of the blockchain take more than that time. Additionally, Table 12 shows that the time complexity of our proposed system is better than all the recent methods, except for Blockchain 3. Blockchain 3 takes the same time complexity as our proposed method. However, the proposed method takes less time than Blockchain 3 because the proposed method uses run-length code to compress data. Additionally, Table 12 shows that all methods need O(n) space complexity to create any number of transactions, where n represents the number of transactions. The following figure shows the amount of time needed by all recent methods and our proposed system to create a specific number of blocks. Figure 5 shows that our proposed method can create many blocks in 1 min. For example, if there are 1000 transactions that happen, we want to create 1000 blocks. In this case, our proposed method will take 1500 s (25 min) to build those blocks. By comparison with other blockchain versions, Blockchain 1 will take 180,000 s (50 h) to create the 1000 blocks. Blockchain 2 will take 14,000 s (4 h) to build the same number of blocks. Blockchain 3 will take 2000 s (34 min) to create 1000 blocks. Our proposed method performs better because it uses run-length code to compress data, so it takes less time to create blocks than other methods. Figure 5 also shows that our proposed method builds any number of blocks in as little time as possible.

Table 12. Comparison between the different versions of blockchain and the proposed system.

Parameters	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Baiju [48]	Asma Khatoon [47]	Proposed System
Smart contracts	No	Yes	Yes	Yes	Yes	Yes
Data secure	Digital currency		Finical	Medical data	Medical data	Medical data
Scalability	No	No	No	No	No	Yes
Level of decentralization	Low	High	High	High	High	High
Interoperability	No	No	Yes	No	No	Yes
Human readable address	No	Yes	No	Yes	Yes	Yes
Deposit time	10-15 min	5 min	Near to instance	5 min	5 min	Near to instance
Data privacy	No	No	Yes	No	No	Yes
Transaction time	2–4 min	14 s	2 s	14 s	14 s	1–2 s
Time complexity	O(n^2)	$n \log n$	O(n + d)	$n \log n$	$n \log n$	O(n + d)
Space complexity	O(n)	O(n)	O(n)	O(n)	O(n)	O(n)

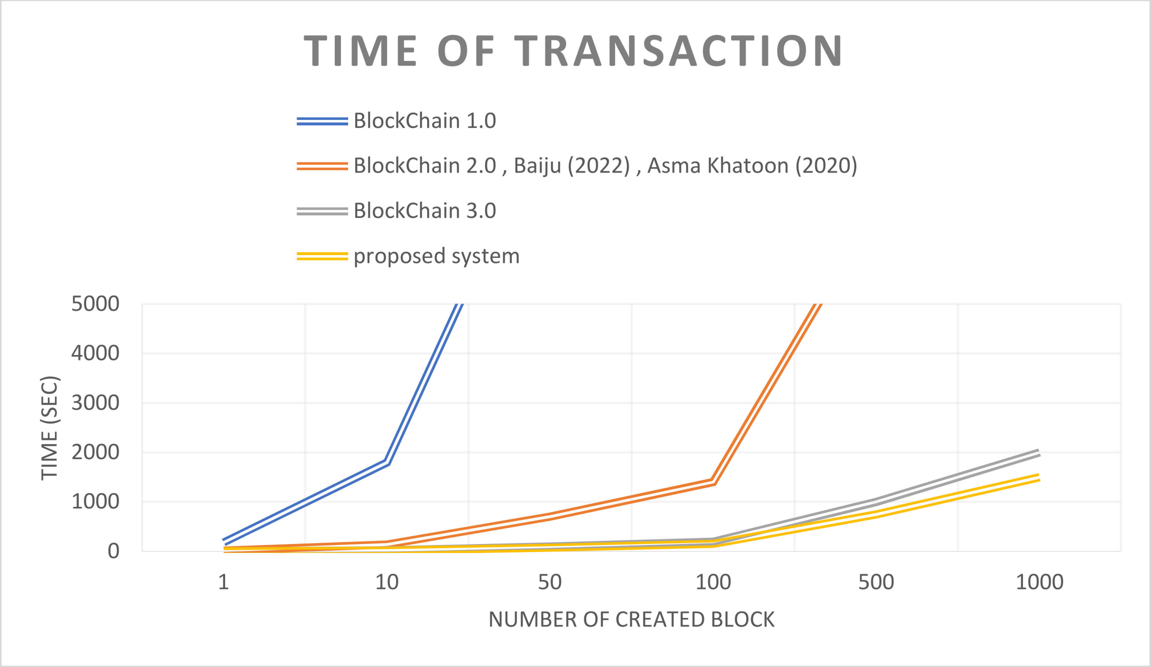

Figure 5. Time of transaction.

Figure 6 shows the time that each method takes to transfer money from patient to physician. Figure 6 shows the comparison between all the recent methods and our proposed method when many deposit processes need to happen at the same time. For example, if 500 deposit processes are needed, Blockchain 1 needs 6250 s to transfer the money from 500 patients to 500 physicians. Blockchain 2 needs 2500 s to transfer money from 500 patients to 500 physicians. Blockchain 3 and our proposed system take 8 s to send the money from 500 patients to 500 physicians. Figure 6 shows that the time that the proposed method takes to deposit money into a physician's wallet is similar to that of the blockchain 3, but it is less time than the other versions take.

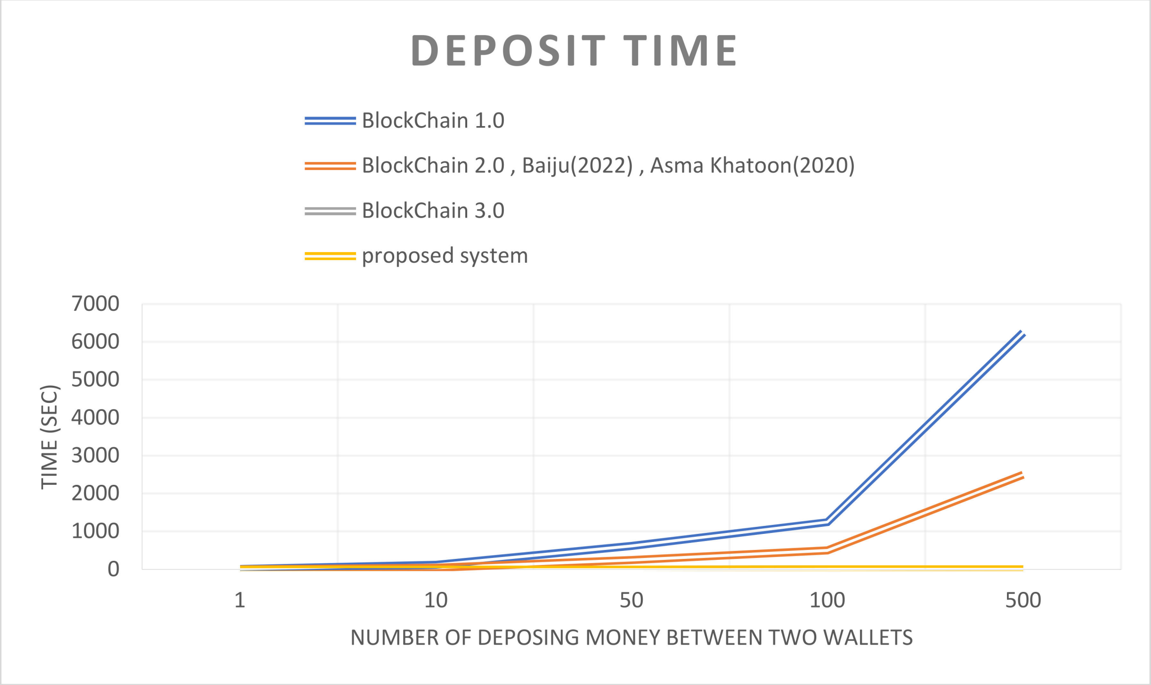

Figure 6. Deposit time comparison between proposed method and blockchain versions.

5. Conclusions

In this paper, we introduced a new technique to make patient data secure and private by using blockchain with smart contracts to prevent hackers from stealing or modifying the data. Smart contract implementation in the healthcare field was used with blockchain for the purpose of making management systems to store medical data or trial experiments. However, in this work, we used smart contracts to guarantee the rights of the doctor according to his efforts in treating the patient. Our proposed private medical blockchain algorithm takes O(n) if we have data that do not start with zero, where *n* is the size of the hash function. However, it takes O(n + d) if the hash of the block starts with a d number of consequence zeros that the hash contained at the beginning. The medical smart contract does not take much time to create since it takes O (1) time complexity for the creation stage. Our proposed method has one problem, namely that the patient must wait until the physician sends the treatment to him. Therefore, in future work, we intend to use a deep learning algorithm to design and build a robot that replaces physicians. This system can send the treatment to the patient without returning to the doctor or sending data over the Internet. Additionally, we intend to make patients and physicians able to send images through our system, so we will develop a technique that hides data from said images [50].

Author Contributions: Conceptualization, I.S.F., S.E. and A.E.T.; methodology, I.S.F., W.A., M.E., S.E. and A.E.T.; software, I.S.F., W.A., M.E., S.E. and A.E.T.; validation, I.S.F., W.A., M.E., S.E. and A.E.T.; formal analysis, I.S.F., W.A., M.E., S.E. and A.E.T.; investigation, I.S.F., W.A., M.E., S.E. and A.E.T.; writing—original draft preparation, W.A., 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., S.E. and A.E.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
2. Trabelsi, S. Monitoring leaked confidential data. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019.
3. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access* **2022**, *10*, 12345–12364. [CrossRef]
4. 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]
5. Laghari, A.A.; Wu, K.; Laghari, R.A.; Ali, M.; Khan, A.A. A review and state of art of Internet of Things (IoT). *Arch. Comput. Methods Eng.* **2022**, *29*, 1395–1413. [CrossRef]
6. El-den, B.M. Provable Chaotically Authenticated Encrypted Biomedical Image Using OFDM Transmission. *Fusion Pract. Appl.* **2022**, *9*, 8–18. [CrossRef]
7. Atassi, R.; Alhosban, F.; Dordevic, M. A New Data Fusion Model for Medical Image Encryption in IoT Environment. *Fusion Pract. Appl.* **2022**, *8*, 16–26. [CrossRef]
8. Available online: https://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php (accessed on 7 November 2022).
9. Hughes, F.; Morrow, M.J. Blockchain and health care. In *Policy, Politics, & Nursing Practice*; SAGE Publications: Los Angeles, CA, USA, 2019; Volume 20, pp. 4–7.
10. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
11. Emira, H.H.A. Authenticating IoT devices issues based on blockchain. *J. Cybersecur. Inf. Manag.* **2020**, *1*, 35. [CrossRef]
12. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
13. Jaramillo, K.P.; Quilambaqui, J.P.; Yanez, J.M.Q. Blockchain in Healthcare from a Neutrosophic Analysis. *Int. J. Neutrosophic Sci.* **2022**, *18*, 177–188. [CrossRef]
14. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
15. Atassi, R.; Alhosban, F. Fusion Optimization and Classification Model for Blockchain Assisted Healthcare Environment. *Fusion Pract. Appl.* **2022**, *9*, 62–73. [CrossRef]
16. Available online: https://www.capgemini.com/resources/blockchain-a-healthcare-industry-view/ (accessed on 25 June 2018).
17. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
18. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef]
19. Widenius, M.; Axmark, D. *MySQL Reference Manual: Documentation from the Source*; O'Reilly Media, Inc.: Sevastopol, CA, USA, 2002.
20. Available online: https://www.healthcare.digital/single-post/2018/05/26/Blockchain-An-opportunity-to-address-many-complex-challenges-in-Healthcare (accessed on 30 June 2018).
21. McConaghy, T.; Marques, R.; Müller, A.; de Jonghe, D.; McConaghy, T.; McMullen, G.; Henderson, R.; Bellemare, S.; Granzotto, A. Bigchaindb: A Scalable Blockchain Database. White Paper BigChainDB. 2016, Volume 2016. Available online: https://gamma.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf (accessed on 14 November 2022).
22. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 112–125.
23. Mainelli, M.; Smith, M. Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *J. Financ. Perspect.* **2015**, *3*, 38–58.
24. Walsh, L.; Akhmechet, V.; Glukhovsky, M. *Rethinkdb-Rethinking Database Storage*; Hexagram 49, Inc.: Mountain View, CA, USA, 2009.
25. Golosova, J.; Romanovs, A. Overview of the blockchain technology cases. In Proceedings of the 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 10–12 October 2018.
26. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. Available online: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (accessed on 5 October 2021).
27. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016.

28. Watanabe, H.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J. Blockchain contract: Securing a blockchain applied to smart contracts. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–11 January 2016.
29. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–2.
30. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
31. Portmann, E. *Rezension Blockchain: Blueprint for a New Economy*; Springer: Berlin/Heidelberg, Germany, 2018.
32. Irving, G.; Holden, J. How Blockchain-Timestamped Protocols Could Improve the Trustworthiness of Medical Science. *F1000Research* **2016**, *5*, 222. [CrossRef]
33. McKernan, K.J. The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources. *Mitochondrial DNA Part A* **2016**, *27*, 4518–4519. [CrossRef]
34. Jenkins, J.; Kopf, J.; Tran, B.Q.; Frenchi, C.; Szu, H. Bio-mining for biomarkers with a multi-resolution block chain. Independent Component Analyses, Compressive Sampling, Large Data Analyses (LDA), Neural Networks, Biosystems, and Nanoengineering XIII. *Int. Soc. Opt. Photonics* **2015**, *9496*, 139–148.
35. Baxendale, G. Can blockchain revolutionise EPRs? *ITNow* **2016**, *58*, 38–39. [CrossRef]
36. Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
37. Witchey, N.J. Healthcare Transaction Validation Via Blockchain Proof-of Work, Systems and Methods. U.S. Patent 20150332283A1, 19 November 2019.
38. Kuo, T.-T.; Ohno-Machado, L. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv*, 2018; arXiv:1802.01746.
39. Ekblaw, A.; Azaria, A. MedRec: Medical Data Management on the Blockchain. Viral Communications [Internet]. 2016. Available online: https://viral.media.mit.edu/pub/medrec (accessed on 5 January 2022).
40. Nugent, T.; Upton, D.; Cimpoesu, M. Improving Data Transparency in Clinical Trials Using Blockchain Smart Contracts. *F1000Research* **2016**, *5*, 2541. [CrossRef] [PubMed]
41. Vayena, E.; Brownsword, R.; Edwards, S.J.; Greshake, B.; Kahn, J.P.; Ladher, N.; Montgomery, J.; O'Connor, D.; O'Neill, O.; Richards, M.P.; et al. Research led by participants: A new social contract for a new kind of research. *J. Med. Ethics* **2016**, *42*, 216–219. [CrossRef] [PubMed]
42. Smith, S.B. Method and System to Use a Block Chain Infrastructure and Smart Contracts to Monetize Data Transactions Involving Changes to Data Included into a Data Supply Chain. U.S. Patent 20150379510A1, 31 December 2015.
43. Savelyev, A. Contract law 2.0: 'Smart'contracts as the beginning of the end of classic contract law. *Inf. Commun. Technol. Law* **2017**, *26*, 116–134. [CrossRef]
44. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
45. Balcerzak, A.P.; Nica, E.; Rogalska, E.; Poliak, M.; Kliěstik, T.; Sabie, O.-M. Blockchain Technology and Smart Contracts in Decentralized Governance Systems. *Adm. Sci.* **2022**, *12*, 96. [CrossRef]
46. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 1–7. [CrossRef] [PubMed]
47. Sharma, A.; Tomar, R.; Chilamkurti, N.; Kim, B.-G. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics* **2020**, *9*, 1609. [CrossRef]
48. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [CrossRef]
49. 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.
50. Kanwal, S.; Tao, F.; Almogren, A.; Ur Rehman, A.; Taj, R.; Radwan, A. A robust data hiding reversible technique for improving the security in e-health care system. *Comput. Model. Eng. Sci.* **2022**, *134*, 201–219. [CrossRef]