electronics

MDPI

Article

Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things

Aniruddha Bhattacharjya [1], Kamil Kozdrój [2], Grzegorz Bazydło [3] and Remigiusz Wisniewski [3,*]

[1] Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, Andhra Pradesh, India
[2] Perceptus Sp. z o.o., 66-002 Zielona Góra, Poland
[3] Division of Information Systems and Cybersecurity, Institute of Control & Computation Engineering, University of Zielona Góra, 65-417 Zielona Góra, Poland
* Correspondence: r.wisniewski@issi.uz.zgora.pl

Abstract: The Internet of Medical Things (IoMT) global market has grown and developed significantly in recent years, and the number of IoMT devices is increasing every year. IoMT systems are now very popular and have become part of our everyday life. However, such systems should be properly protected to preventing unauthorized access to the devices. One of the most popular security methods that additionally relies on real-time communication is Blockchain. Moreover, such a technique can be supported by the Trusted Third Party (TTP), which guarantees data immutability and transparency. The research and industrial community has predicted the proliferation of Blockchain-based IoMT (BIoMT), for providing security, privacy, and effective insurance processing. A connected environment comprises some of the unique features of the IoMT in the form of sensors and devices that capture and measure, recognize and classify, assess risk, notify, make conclusions, and take action. Distributed communication is also unique due to the combination of the fact that the Blockchain cannot be tampered with and the Peer-to-Peer (P2P) technique, especially compared to the traditional cloud-based techniques where the reliance of IoMT systems on the centralized cloud makes it somewhat vulnerable. This paper proposes a Blockchain-based technique oriented on IoMT applications with a focus on maintaining Confidentiality, Integrity, and Availability (the CIA triad) of data communication in the system. The proposed solution is oriented toward trusted and secure real-time communication. The presented method is illustrated by an example of a cloud-based hospital application. Finally, the security aspects of the proposed approach are studied and analyzed in detail.

Keywords: blockchain; Blockchain-based Internet-of-Medical-Things (BIoMT); CIA triad; Internet-of-Medical-Things (IoMT); Peer-to-Peer (P2P); secure; trusted; Trusted Third Party (TTP)

Citation: Bhattacharjya, A.; Kozdrój, K.; Bazydło, G.; Wisniewski, R. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics* **2022**, *11*, 2560. https://doi.org/10.3390/electronics11162560

Academic Editors: Juan Antonio López Ramos, Antonio David Escobar Molero and José Antonio Álvarez Bermejo

Received: 26 July 2022
Accepted: 13 August 2022
Published: 16 August 2022

1. Introduction

Allied Market Research published research [1] that shows the IoMT global market was USD 41.17 billion in 2020 and is projected to grow to USD 187.6 billion in 2028. It is predicted that the blockchain-based IoMT will proliferate in providing security, privacy, and effective insurance processing in the present era [2–9]. IoMT offers a connected environment of sensors along with related devices, which function in capturing and measuring, recognizing and classifying, assessing risk, informing, making decisions, and taking actions. In the hospital environment, the use of the IoMT contributes to the use of smart and connected equipment for better inventory management, real-time location services, resource utilization, and patient/personnel flow tools [2,3,6]. With the modern technological evolutions in the IoMT, without the need of visiting a hospital, patients' clinical data can be remotely monitored and processed with real-time data systems. At any moment, these data can be relocated to the cloud for future use [10–13].

One of the main challenges that is faced by the designers of the IoMT is especially related to the protection of the system and real-time communication between the connected

devices [14,15]. The IoMT systems are very often crucial for human life (especially in the area of healthcare and monitoring systems); thus, they should be extremely trustworthy and secure, preventing unauthorized access. One possible solution to this problem relies on Blockchain technology [16–18]. This technique is a tamper-proof digital ledger with a secure Peer-to-Peer (P2P) communication feature [5,7–9], and has already been successfully utilized both in business and personal applications [19–21]. The initial "chain of blocks" idea appeared in 1991 [22] when this technology was used to mark documents with timestamps. In recent years, Blockchain has become very popular due to its application in cryptocurrencies (formerly Bitcoin [23] in 2009). However, its architecture offers wide possibilities for applications in other areas of human life, including healthcare systems [24–28], and trusted and secure durable medium e-services [29]. Besides the security aspect, blockchain can also be used in trusted transactions, by the introduction of the TTP to the applied system. This solution is very often applied in modern blockchain-based techniques in order to prevent tampering with the blockchain database [30–33]. Moreover, it permits immutability and transparency of the data stored within the system [34,35]. Conversely, TTP can be problematic because each user of the system should agree on its use. Nevertheless, let us point out that it is possible to apply blockchain technology to empower communication among non-trusting members devoid of the third party [11].

When it comes to the application of Blockchain technology to the IoMT, such a combination may bring several measurable benefits, mainly in the healthcare area. It seems that IoMT architecture employing Blockchain technology is much better than cloud-based IoMT architecture because it enables a global view of the patient's medical records in an efficient, verifiable, and permanent way. The security of the information in cloud-based IoMT architecture is the foremost problem in real-time data communication in connected networks [10–13]. Nevertheless, the scientific problem relates to the reliance of IoMT architectures on the centralized cloud, resulting in vulnerability. Therefore, this paper deals with the above problems, in particular, those related to the drawbacks of cloud-based IoMT architecture and current centralized IoMT systems (e.g., in hospitals).

The main contribution proposed of this paper can be summarized as follows:

- A holistic overview of the currently applied Blockchain-based methods oriented on IoMT;
- proposition of a novel trusted and secure Blockchain-based architecture for Internet-of-Medical-Things (BIoMT architecture);
- analysis and discussion of the security aspects of the proposed solution with the application of the Elliptic Curve Digital Signature Algorithm (ECDSA);
- implementation and experimental verification of the proposed BIoMT architecture with the use of the MultiChain platform.

The remainder of the paper is structured as follows. Section 2 presents Blockchain technology's unique benefits for IoMT architectures. Section 3 describes in detail the proposed BIoMT architecture. The implementation and experimental verification of the proposed approach are presented in Section 4, and Section 5 concludes the paper. Table 1 gives the abbreviations used in the paper.

Table 1. Abbreviations used in the paper.

Name	Abbreviation
Address Resolution Protocol	ARP
Blockchain-based Internet-of-Medical-Things	BIoMT
Blockchain-based architecture for Internet-of-Medical-Things	BIoMT architecture
Confidentiality, Integrity, and Availability	CIA triad
Discrete Logarithm Problem	DLP
Distributed Denial-of-Service	DDoS
Elliptic Curve	EC
Elliptic Curve Cryptography	ECC

Table 1. *Cont.*

Name	Abbreviation
Elliptic Curve Digital Signature Algorithm	ECDSA
Elliptic Curve Discrete Logarithm Problem	ECDLP
Industrial Internet-of-Things	IIoT
Internet-of-Medical-Things	IoMT
Internet-of-Things	IoT
Interplanetary File System	IPFS
Man-in-the-Middle	MITM
Merkle Hash Tree	MHT
Proof-of-Work	PoW
Public Key Cryptography	PKC
Public Key Infrastructure	PKI
Peer-to-Peer	P2P
Trusted Third Party	TTP

2. Blockchain Technology's Unique Benefits for IoMT Architectures

This section presents the most important unique Blockchain technology advantages regarding its application in present IoMT systems [5–9]. It seems that BIoMT can underpin a revolution in the field of IoMT. The following capabilities of the Blockchain make it very suitable as a foundational element of IoMT solutions (each of these are discussed later in this section):

- trustworthy and secure solution;
- decentralized, trustless nodes;
- autonomous functioning.

Blockchain technology has the unique ability to maintain the trusted ledger of all transactions that are taking place in real-time in the network. Therefore, trustworthiness is the main advantage of the huge scalability in the IoT and IoMT networks of billions of connected devices. To build trustworthiness in IoMT, Blockchain features such as trust, immutability, and verifiability can be applied [36–39].

Blockchain is usually implemented as a public network. This means that all participating members can see transactions stored within Blockchain; however, the actual content of the personal transaction (block content) is secured by the user's private key. Moreover, Blockchain can be treated as a public ledger of all transactions maintained by the different decentralized nodes. Due to decentralization, no single authority is responsible for approving the transactions or setting specific rules for accepting them. In other words, its distributed and consensus mechanism plays an important role in this process of acceptance. Moreover, trust in the solution is a key factor here because, to accept the transaction by all connected nodes, a consensus is needed between them. Consequently, the resulting system is a more resilient ecosystem for connected devices. All the real-time transactions are linked with cryptographic keys and immutable ledgers; therefore, tampering with or removing the stored information is very difficult. Such a tamper-proof system meets several compliance and regulatory necessities of industrial IoT (IIoT) applications and will be useful for IoMT systems too [36–39].

Blockchain is, by definition, secure. Moreover, the cryptographic algorithms used by Blockchain can make the user data more private. The public audit, consensus mechanisms, and timestamps are used for storing the data in an immutable manner. This enables the architecture to maintain the CIA (Confidentiality, Integrity, and Availability) triad. Conventional information security practices impose the enactment of the principles of the CIA triad. Blockchain technology uses the unique operational distributed database, which is the form of data storage for all the nodes. An excellent feature is that this structural distributed database stores the data in an encrypted form, which is validated using various checks such as Merkle Hash Tree (MHT) and Elliptic Curve Cryptography (ECC). Moreover, researchers continue to implement Public Key Infrastructure (PKI). Such

solutions are usually based on the ECC or on the techniques that involve primes (e.g., RSA cryptosystem [40,41]). In the case of Blockchain-based systems, PKI increases the security of data management. Furthermore, it is worth mentioning that Man-in-the-Middle (MITM) attacks are less possible if Blockchain technology is used, because the Blockchain is tamper-proof and no malicious actor can alter or manipulate the data. This is due to the fact that data is stored in multiple locations, rather than a single location [36–39]. Moreover, the potential interception of a single thread of communication poses no danger [42].

Regarding the IoMT, data produced by such systems (including smart medical devices) can be maintained and kept secure by the Blockchain. This means that IoMT devices may be able to work independently without the need for a centralized authority. Blockchain enables a decentralized P2P network where all the transactions are verified and validated by a consensus among peers. Therefore, in principle, this network is also trust-free, as there is no requirement for trusting each other, which can be beneficial for IoMT systems.

Furthermore, Blockchain makes trust-free P2P messaging possible, which is also required for IoMT. The Blockchain network is resilient to failures due to its decentralized P2P network. It is indeed an immutable and durable ledger, so after consensus among the peers, when all the real-time transactions are recorded in the Blockchain, then no alterations or deletions are possible.

Finally, Blockchain technology can be very useful for tracking connected medical devices, resulting in a quicker distribution of transactions along with the coordination between the connected devices. In other words, it can contribute to major savings for hospitals and the whole healthcare sector.

In conclusion, the main advantages of using Blockchain technology in IoMT can be summarized as:

- Trustworthiness in IoMT.
- Blockchain features such as trust, immutability, and verifiability can be applied in present IoMT systems.
- Due to decentralization, no single authority will be responsible for approving the transactions or setting specific rules for accepting them in the IoMT system with this technology.
- The distributed and consensus mechanism plays an important role in this process of acceptance.
- The tamper-proof system of the Blockchain technology meets several compliance and regulatory necessities of both industrial IoT and IoMT systems.
- Security is enhanced by Blockchain technology in IoMT systems via the use of cryptographic algorithms.
- The validation process in Blockchain uses various checks such as MHT and ECC, and is another reason for more security.
- The CIA triad is maintained using Blockchain technology in IoMT.
- Dangerous MITM attacks are less possible with the use of Blockchain technology, due to features such as being tamper-proof and malicious actors being unable to alter or manipulate the data. We know that the data is stored in multiple locations.
- Blockchain's decentralized P2P network is highly advantageous as all the transactions are verified and validated by a consensus among peers; as a result, there is no requirement for trusting each other, thus enabling trust-free networks in IoMT.
- Feature such as tracking by use of Blockchain technology results in faster transactions in IoMT systems. Significant economic benefits exist for hospitals and allied industries.

Clearly, it is very well understood that the use of Blockchain technology may enhance many aspects such as security, efficiency, trustworthiness, and privacy due to the maintenance of P2P networking.

3. The Proposed Blockchain-Based IoMT Architecture

Here we present the proposed IoMT architecture. The technique is based on Blockchain technology. As discussed earlier, in the healthcare area the contribution of IoMT can be

the development of real-time connected and smart equipment, which can be used for better inventory management and resource utilization, along with location services and patient and personnel flow tools [7]. It is well understood that patient use of IoMT devices reduces hospital visits to a minimum, and patients' clinical data can be remotely monitored, analyzed, and gathered with real-time data systems [2–4,6]. These data can also be stored in the cloud for future use. Of course, such a huge amount of sensitive data must be protected against unauthorized access or tampering.

Figure 1 shows an exemplary cloud-based hospital application architecture in the present IoMT system [7,10–13]. The IoMT network is able to incorporate all smart connected things as a part of the IoMT system. However, it is a well-known fact that, in a centralized cloud-based system, single-point failure (especially key points) is a major weakness.

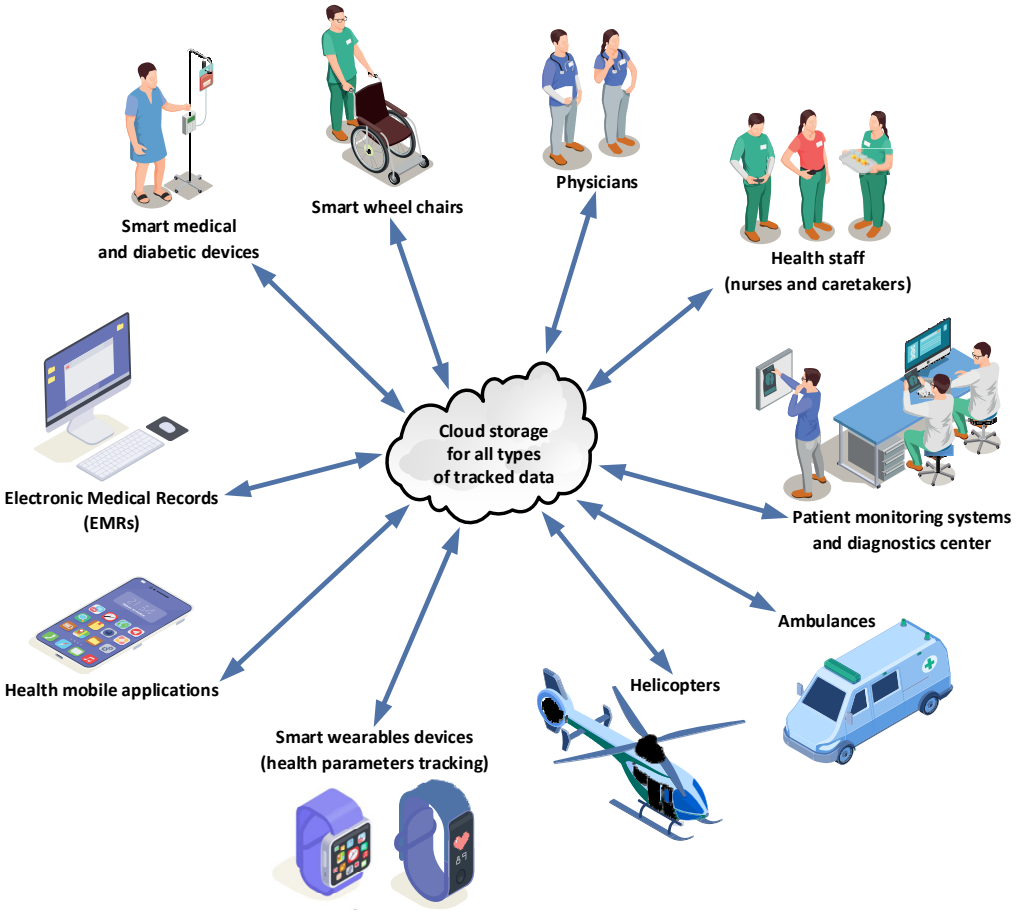

Figure 1. Cloud-based hospital application architecture in the present IoMT system.

At present, these cloud-based architectures manage threats such as Distributed Denial-of-Service (DDoS) attacks, Address Resolution Protocol (ARP) spoofing attacks, various phishing and configuration threats, and network congestion. The weak point of the centralized, client-server-based architecture with a centralized control system is that, if the centralized system collapses, then the whole system (with connected devices) will stop functioning properly. Thus, there is a need for a new kind of secure distributed communication. Blockchain technology's advantages can help to resolve these problems as discussed in the previous section.

Figure 2 shows the proposed IoMT architecture with the use of Blockchain technology. To uphold accountability and auditability of the network, a private Blockchain can be used in the proposed BIoMT architecture, which will help provide authentic users with access to

the network. The data kept on the Blockchain are signed, so the responsibility lies on the users—anyone who gains access to the data is responsible for their actions taken on it.

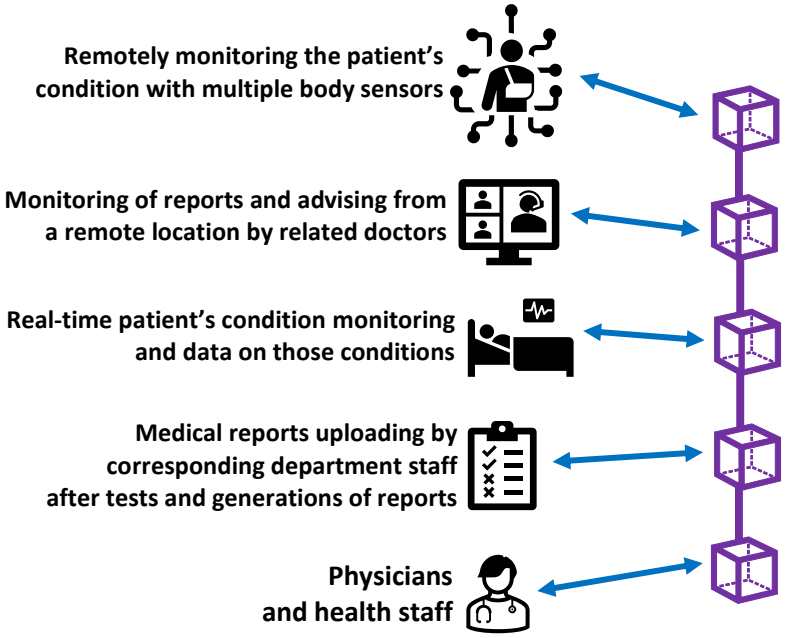

Figure 2. The proposed IoMT architecture with the use of Blockchain technology.

According to Figure 2, it is clear how the Blockchain technology's advantages discussed earlier can be implemented in BIoMT to maintain data of the patient, monitor reports and the patient's condition in real-time systems, and securely maintain medical test reports. The IoMT architecture with the use of Blockchain technology (BIoMT) is a unique and novel approach for the protected transmission of all patient health reports to safeguard medical data. It is well understood that, being a decentralized architecture, the Blockchain-based methodology can resolve several problems of the centralized cloud architectures. Figure 3 is a micro-detailed diagram to show how the Proof-of-Work (PoW) consensus protocol is used in the proposed model, starting from adding a new report in the patient medical file to the formation stored in the chain.

The proposed BIoMT architecture shown in Figure 3 is a unique and novel solution for the protected transmission of all patients' health reports, with the ultimate goal of securing medical data. It is well understood that, being a decentralized architecture, the Blockchain-based methodology can resolve several problems with centralized cloud architectures.

The proposed Blockchain-based IoMT architecture is able to handle highly sensitive security and privacy concerns due to the principles of the Blockchain technology's inherent security features. Hence, the use of the Blockchain will ensure the security of patients' clinical records in practice and will be able to grant tamper-free open access to all nodes in the IoMT network.

The possibility of using enhanced security is another goal of the proposed BIoMT architecture. ECDSA [43] is already in use in several Blockchain-based architectures and Bitcoin [44,45] (see Section 4.2 for more details). Nonetheless, some security aspects and efficiency are a challenge for these solutions [46,47].

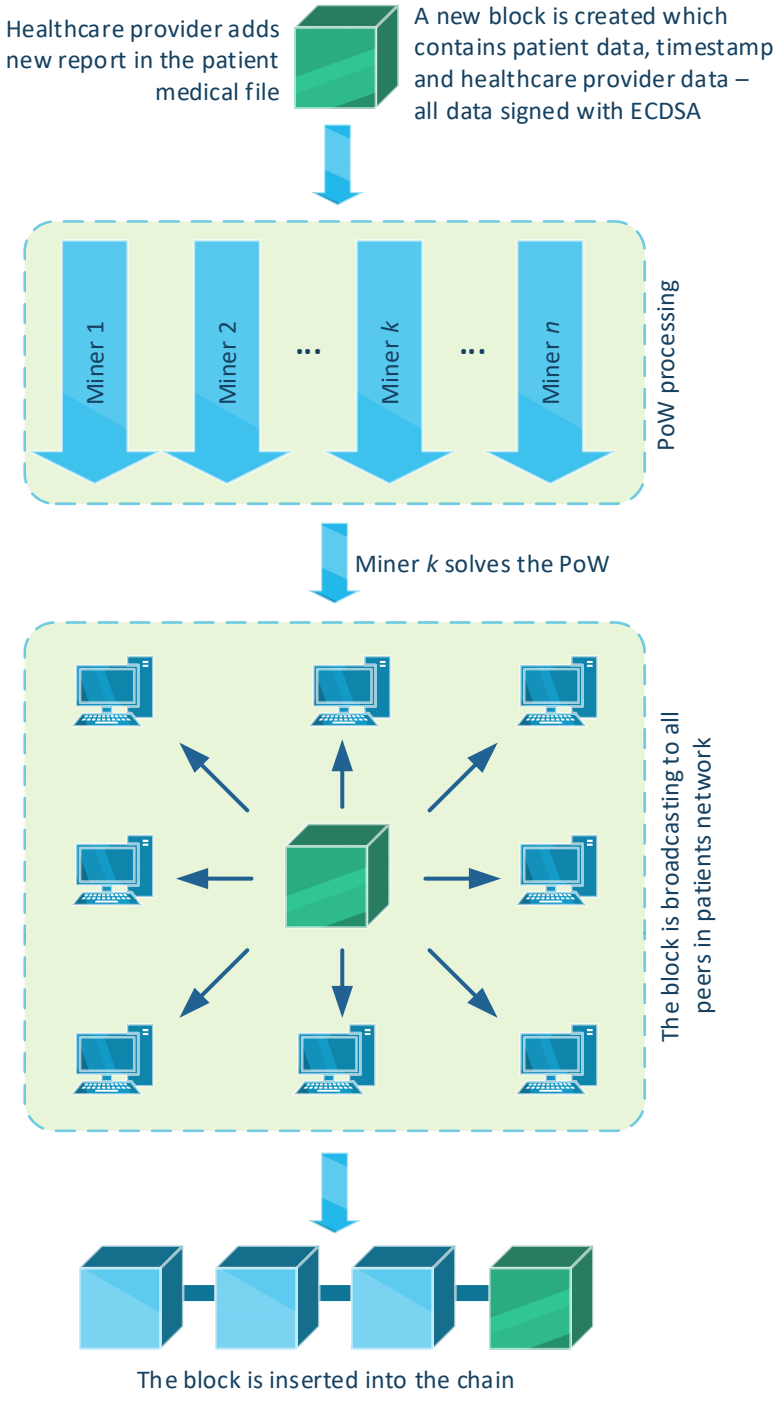

Figure 3. The PoW consensus protocol in the proposed BIoMT architecture.

4. Experimental Verification of the Proposed Solution

The proposed trusted and secure blockchain architecture was verified experimentally. To achieve this, a real-world case of the IoMT database was prototyped. This section describes the performed experimental verification. Firstly, the structure of the used blockchain is shown. Next, the applied signing technique is described in detail. Finally, the results achieved are presented and discussed.

4.1. The Blockchain Structure

The proposed blockchain structure is presented in Figure 4. Several fields of the presented database ("index", "timestamp", etc.) are enforced by the blockchain structure itself, whereas the others are explained in this subsection.

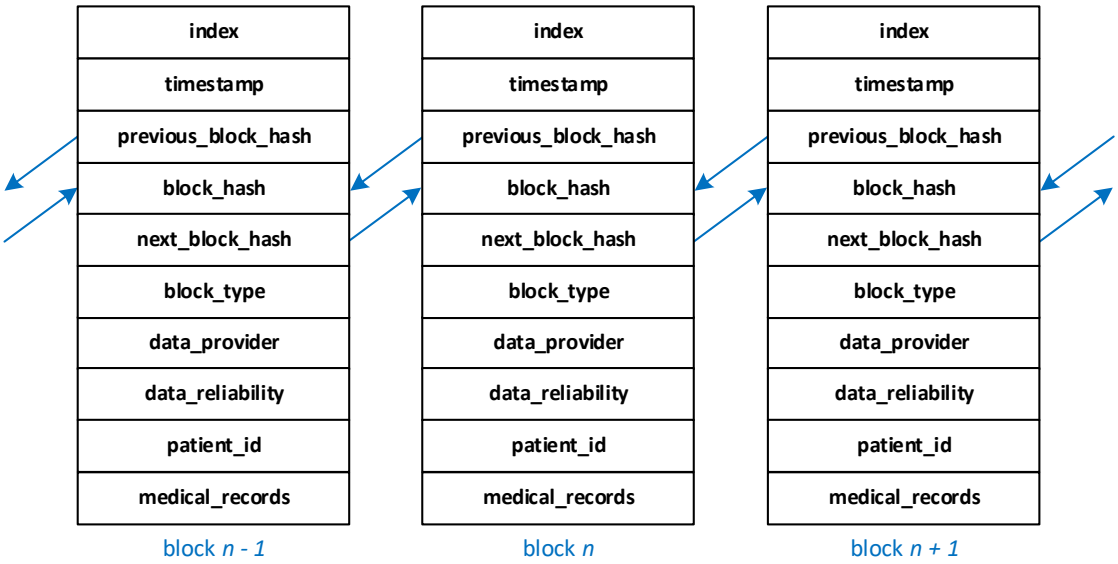

Figure 4. The proposed structure of the blockchain.

It is assumed that the network can keep many types of blocks (specified with a numeric field "block_type"), e.g., the value "1" means that the block contains data generated by the IoMT device, the value "2" means that data comes from hospital patient monitoring system, and the value "3" denotes the data contains the medical report. It should be noted that the proposed approach is not limited to these three types of blocks and can be freely extended to any number of block types.

The subsequent field "data_provider" denotes the source of the data, e.g., the identification number of the IoMT device and the department name (in the case of a medical report).

Medical data can be provided by specialized medical devices (e.g., blood pressure monitors, glucometers) and smart bands or IoT/IoMT sensors, which have become very popular in recent years. The latter are not certified medical devices, which means that the medical data collected by them are uncertain and not reliable for health staff; nonetheless, such devices may be useful in the overall assessment of the patient's health and should be kept in the blockchain. Therefore, the field "data_reliability" can be very useful to assess the reliability of the data.

The next field, "patient_id", specifies the patient or indicates (the value "0") that the data do not relate to a single patient (e.g., in the case of medical reports). The last field is intended for the actual medical records, patient data, healthcare reports, etc.

4.2. Signing Data with ECDSA

It is well known that cybersecurity attacks occur, such as DDoS, ARP spoofing attacks, various phishing and configuration threats, and network congestion, on the present CPS, IoT, and IoMT architectures used in Industry 4.0 applications [36–39]. These attacks are very dangerous to the security of the CIA triad of data. Moreover, as a whole, these attacks can have significant impacts on the efficient functioning of these systems. Industry 4.0 applications are struggling to deal with the CIA triad, along with access control and authorization. One of the reasons for this could be the increasing automation of these systems, resulting in new kinds of cyberattacks and consequently increasing substantial financial losses. Therefore, many cryptocurrencies and Blockchain-based systems use

ECDSA [43–45]. In this section, we propose the ECDSA, which is used in many Blockchain-based systems and can be successfully applied as a part of the proposed BIoMT architecture, especially for the signing of medical records and patient medical data.

Let us start with the general analysis of the Elliptic Curve (EC) technique. According to [48], the Elliptic Curve method consists of the following steps:

1. Let $GF(f)$ be a prime field.
2. Then let $s, t \in GF(f)$ be constant such that $4s^3 + 27t^2 \neq 0$.
3. An EC $E(s, t)$, over $GF(f)$, is considered the set of points $(x, y) \in GF(f)$ which fulfil Equation (1), called the "short Weierstrass form" [49]:

$$y^2 = x^3 + Sx + T \quad (1)$$

where S and T are constant.

Furthermore, it is well known that if G is a group, then the Elliptic Curve Discrete Logarithm Problem (ECDLP) is used to find the integer a for group elements S and T in such a way that $T = aS$ [50].

There is a constant need to search for faster and more computationally efficient cryptographic algorithms, of which ECDSA [43–45] is one. ECDSA was invented in 1992 by Scott Vanstone [43]. As an ANSI standard, it was released in 1999.

The proposed use of ECDSA for signing the medical records (kept in the block in the blockchain) consists of the following steps:

1. Generation of the Key:
   (a) the required chosen EC is well defined over a finite field F_c with the characteristic c, and with a base point $G \in E_c(s, t)$ with an order of n;
   (b) **select** a random integer h such that $1 \leq h \leq n - 1$;
   (c) **compute** $T = h \times G$ and finally, the public key pair is (T, h).
   (d) **the public key pair is (*T*, *h*)**.
2. Generation of the Signature (let m be medical records to be signed):
   (a) **select** an integer k in such a way that $1 \leq k \leq n - 1$,
   (b) **compute** $k \times G = (x1, y1)$,
   (c) **compute** $r = x1 \bmod n$:
   if $r = 0$ **then** select new k.
   (d) **compute** $k - 1 \bmod n$ and $e = h(m)$.
   (e) **compute** $s = p{-}1(e + kr)$:
   if $s = 0$ **then** go to step (2a).
   (f) **pair (*r*, *s*) is the generated signature for the medical records *m***.
3. Verification of the signature (r, s) of medical records m signed by verifier V:
   (a) **verify** (**by** V) whether $r, s \in [1, n - 1]$,
   (b) **compute** $e = h(m)$ and s^{-1},
   (c) **compute** $u = es^{-1} \bmod n$ and $v = rs^{-1} \bmod n$,
   (d) **compute** $w = (x_2, y_2) = uG + vT$:
   if $w = 0$ **then stop**
   else compute $t = x_2 \bmod n$.

   The signature is valid only if $t \equiv r$. Proof of the verification process is in Equation (2):

$$kG = s^{-1}(e + k_r)G \bmod n = s^{-1}eG + s^{-1}r_kG \bmod n = uG + vQ \bmod n \quad (2)$$

Therefore, $uG + vT = kG$ and so $t = r$, which is requisite.

Finally, it is a well-known fact that the cryptographic security of Public Key Cryptography (PKC) based on EC relies on an intractable mathematical problem known as the Discrete Logarithm Problem (DLP) [43,48,51]. Because the EC does not have a sub-exponential-time algorithm to solve ECDLP [43–45], ECDSA can be used to encrypt and sign the data from the IoMT devices before adding it to the blockchain.

There are several threats to present IoMT systems [52], but BIoMT is able to solve MITM and DOS attacks by maintaining the CIA triad or implementing special intrusion detection and prevention systems, as proposed in [52]. Such a solution is capable of discriminating between and automatically mitigating selected cyberattacks by applying machine learning and software-defined networking technologies. Another e-health technique analyzed in [53] proves that using Blockchain technology in electronic health record systems makes health care data more secure and sustainable. It is worth noting that any BIoMT architecture ensures the utmost security and handles privacy threats by applying the Blockchain principles mentioned in Section 2. Therefore, using the Blockchain with ECDSA assures that, in practice, the security of patient clinical records will be able to be openly accessed and remain tamper-free. Moreover, the BIoMT architecture using Blockchain technology together with ECDSA will be able to meet the requirements of the CIA triad regarding data communication in BIoMT systems.

4.3. The Experimental Verification

The proposed BIoMT architecture was implemented using the MultiChain platform [54] and verified experimentally. In our research, the private version of the blockchain is used. This means that access to the blocks stored in the blockchain is possible only with the appropriate access permissions. Moreover, due to security reasons, only one blockchain is generated (data stored in one blockchain decrease the possibility of blockchain manipulation). The blockchain was created on one computer (Intel i7 processor, 16 GB RAM, 250 GB SSD, Windows 10), and a second (with similar technical parameters) was used to access and manage the blockchain. The selected, most important blockchain parameters used in the implementation of the BIoMT architecture are presented in Table 2.

Table 2. Selected blockchain parameters used in the implementation of the BIoMT architecture.

Parameter	Value	Meaning
Chain name	BIoMT	The name of the blockchain.
Blockchain type	Private	The blockchain could be public or private; in the proposed approach the blockchain should not be public, so the chosen type is private.
Chain protocol	Multichain	The protocol could be multichain or bitcoin-style; to use streams, the multichain should be chosen.
Consensus type	Proof-of-Work	Type of consensus used in the blockchain.
Mining diversity	0.3	Determines how many required miners (with the permission “mine”) must participate in the transaction confirmation (0.0 means no constraint, while 1.0 means that every miner must participate).
Mine empty rounds	10	If there are no new transactions, the parameter defines how many empty rounds will be generated (these empty rounds have a positive impact on building a reliable and resilient blockchain).
Number of streams	5	The number of generated streams.
Number of addresses	10	The number of generated addresses (each of the streams can have several publishers/addresses).
Number of blocks	218	The number of generated blocks in the blockchain.
Number of transactions	10,383	The number of generated transactions kept in all blocks.

The implemented blockchain consists of 218 blocks, and more than 10k transactions. A snapshot of 21 examples is presented in the screenshot in Figure 5. As can be seen, there are 17 transactions (marked in blue) that refer to the medical data. Furthermore, there are three transactions (marked in red) that are used to grant permissions. Moreover, there is an additional transaction (marked in grey) that refers to the empty round, and thus it contains no data.

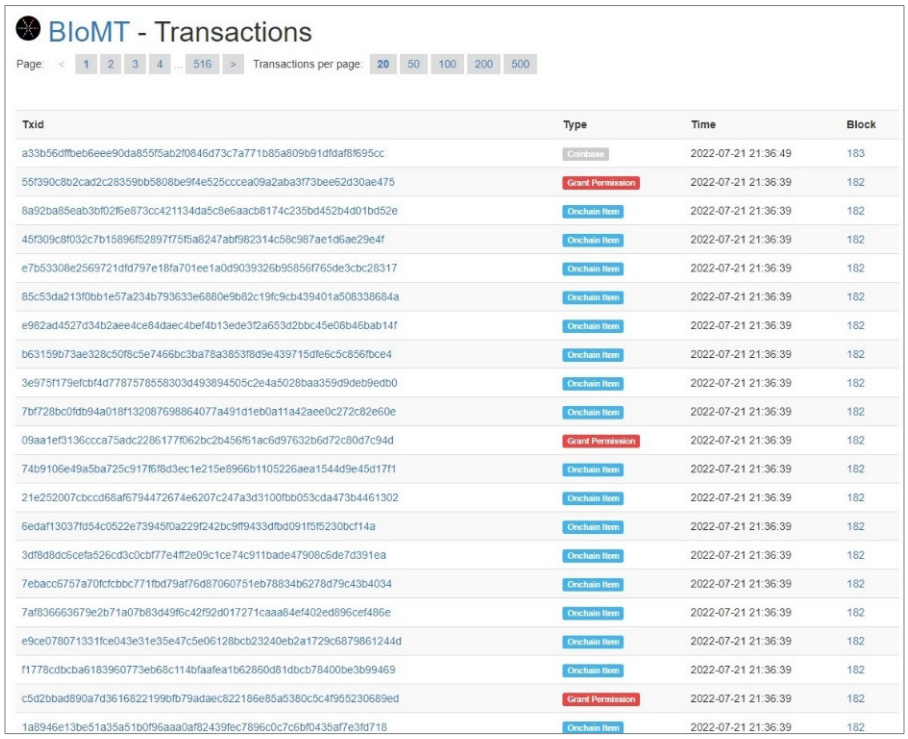

Figure 5. The screenshot of exemplary 21 transactions from the implemented blockchain.

The example content of one selected block is presented in Figure 6. As can be seen, block number 208 contains as many as 14 transactions.

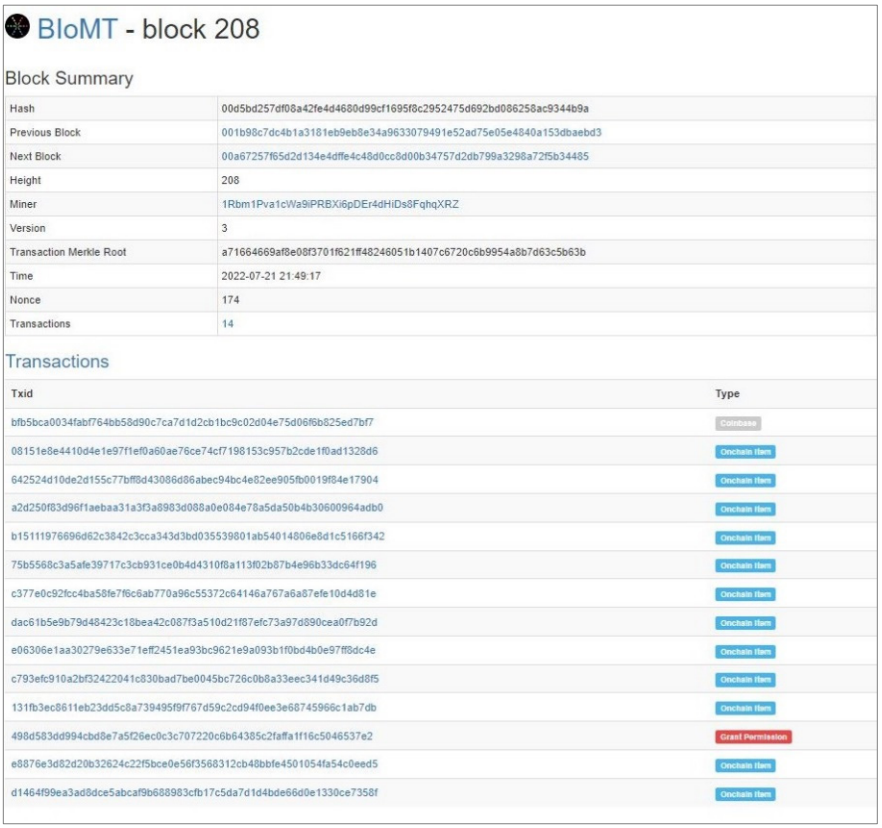

Figure 6. The content of one selected block from the implemented blockchain.

In the implemented BIoMT architecture, five streams are created, and the appropriate numbers of publishers (addresses) for each. Selections are shown in the screenshot in Figure 7.

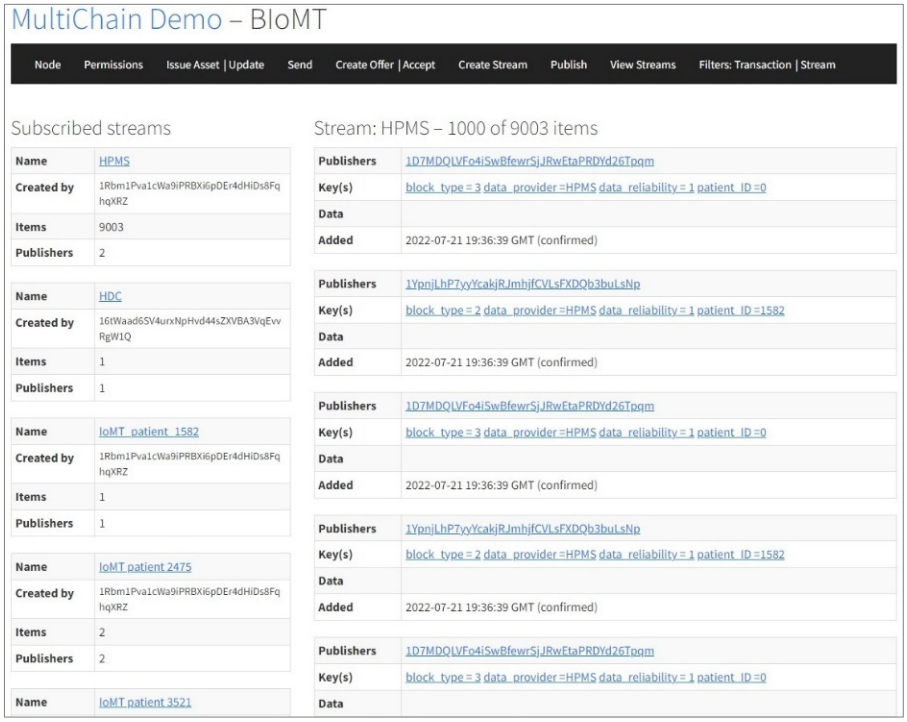

Figure 7. Selected streams with publishers (addresses) from the implemented blockchain.

Finally, there was a need to grant adequate permission to the previously created publishers (addresses). In our implementation we use, among other addresses:

- two addresses with permission "mine", which are assigned to two miners responsible for confirming transactions in the blockchain;
- seven addresses with permission "send", which represent the patient's IoMT devices; one address for one patient's device (e.g., smartphone) with access to the blockchain;
- two addresses with permission "send", which represent the hospital patient monitoring system;
- one address with permission "connect", which represents the hospital diagnostic center (this center has access to all blocks in the blockchain).

Summarizing the performed experimental verification of the proposed BIoMT architecture, the implementation of blockchain works properly and effectively thanks to the use of the MultiChain platform and specially dedicated scripts created by the authors.

4.4. Performance Evaluation

To estimate the performance of the implemented BIoMT architecture, additional research was undertaken. Three selected types of blockchain transactions were chosen, which correspond to typical medical data stored on the blockchain in BIoMT architecture:

- Transaction with data stored in text form. This is a typical transaction to keep information about the patient personal data or simple test results, such as heart rate and pressure measurements. In the research, we use a CSV file that collects data from the National Lung Screening Trial [55].
- Transaction with data stored in PDF format. This kind of transaction is most often used for storing data from various patient examinations such as blood tests and urine tests. These files also contain small pictures such as the company's logo. Moreover, most

often there is also a need for digital signing of the document, and the PDF format is effective for this purpose. In the research, a signed PDF file was used, which contained example outcomes of the patient's blood test.

- Transaction with data stored in graphical format. This type of transaction is often used for storing, for example, x-ray or computed tomography photos, as well as magnetic resonance images or electrocardiograms. In the research, we used an example x-ray image of the patient's chest (the resolution of the image was 2048 × 2048 pixels).

Subsequently, 101 transactions for each type were created. Note that, before storing data in the blockchain, there was a need to convert the files to binary tables. Next, based on the obtained results, the time of creating one transaction was estimated. The estimation was made using the arithmetic mean and the median; the latter is more resistant to erroneous measurements that differ significantly from typical values. The performance evaluation results are presented in Table 3, and the script in Java for this performance evaluation is presented in Appendix A.

Table 3. The performance evaluation results of the selected BIoMT transactions.

Parameter	Transactions with Text Data	Transactions with Signed Mixed (Text and Graphics) Data	Transactions with JPG Data
File format to store data	CSV	PDF	JPG
The size of the file	1,392,133 bytes	516,510 bytes	342,303 bytes
Number of generated transactions	101	101	101
Total time of all generated transactions	21.7924 s	10.5303 s	6.5877 s
Arithmetic mean of 1 transaction generation time	0.2158 s	0.1043 s	0.0652 s
Median of 1 transaction generation time	0.2046 s	0.0906 s	0.0606 s
Number of used blocks used to store all generated transactions	18	7	5
The average number of transactions per block	5.61	14.43	20.20

4.5. Discussion of the Obtained Results

Here we discuss the obtained results. As mentioned in Section 4.3, the practical implementation of the proposed solution was performed with the use of the MultiChain platform. Moreover, a performance evaluation regarding the creation of selected types of blockchain transactions was conducted and is presented in Section 4.4. The obtained results show the great potential of the proposed approach, and the wide selection of potential applications ranging from healthcare and related industries (such as the biomedical or paramedical industries), to the existing and new areas of IoMT and IoT systems (such as the wireless body field, the automotive industry, and the wide range of smart systems that are present in our daily life, e.g., smart homes, smart buildings, and smart cities).

Of course, the proposed approach has several limitations. First, it should be noted that the implementation results were obtained in a laboratory environment rather than in real conditions; thus, not all potential limitations were considered in the research. Moreover, several popular cyberattacks (e.g., tampering, sniffing, unauthorized access, MITM, DDoS, and ransomware [56]) have not been analyzed and tested on the proposed solution.

Furthermore, the implemented blockchain is rather small—it contains "only" 10 thousand transactions (e.g., in the Bitcoin blockchain, from 3.3 to 7 new transactions are created every second, which results in over 10 million new transactions per month [57]). Nonetheless, even such a small size of the blockchain allowed for experimental verification of the proposed approach and the evaluation of its usefulness. The validation of the implemented BIoMT architecture included a manual analysis of several dozen randomly

selected transactions and blocks. All analyzed blocks and transactions turned out to be correctly generated. Moreover, during the performance evaluation, a comparison of the original PDF file with the one downloaded from the blockchain was performed. The signature verification for both files was also successful.

Finally, the used implementation platform (MultiChain) has also several limitations, such as limiting the size of stored data in one blockchain transaction to 2 MB. If there is a need to store larger data, off-chain technology must be used, e.g., external databases or distributed storage systems such as Interplanetary File System (IPFS) technology [58].

To summarize the above, it should be noted that the performed experiments confirmed the advantages of applying Blockchain technology to the IoMT systems. Moreover, the presented blockchain structure can be treated as a template, which may be adapted and adjusted to the real solutions based on the real requirements (which often result from the unique and specific requirements of a given hospital or other medical institution).

5. Conclusions

In this paper, a novel BIoMT architecture is proposed. The advantages of Blockchain technology in IoMT architectures are also analyzed and discussed. The presented BIoMT architecture can be used to address problems occurring in current cloud-based IoMT solutions. Decentralized BIoMT architecture may be a response to the problem of failure of the main server or other single-point failures. Moreover, the trust and secure Blockchain technology makes the BIoMT architecture tamper-proof, and the presented PoW consensus mechanism increases the security level of patients' clinical records and enables tamper-free open access to all nodes in the BIoMT network.

The proposed Blockchain-based IoMT architecture can be applied to other areas of IoMT, for example, smart hospitals, nursing homes, and allied industries such as biomedical or paramedical industries, in addition to new and existing areas of IoT such as wearable sensors, thew automotive industry, or smart systems.

It seems that ECDSA is now one of the most prominent solutions for use in cryptocurrencies and Blockchain-based architectures. It is well known that the cryptographic security of PKC based on EC depends on an intractable mathematical problem called DLP. However, EC does not have a sub-exponential-time algorithm to solve ECDLP. As a result, the security of the BIoMT is stronger than that of the normal cloud-based IoMT architecture. Only the backdoors in EC are a major problem; thus, in the near future, a research direction may be solving this issue and making ECDSA more efficient and secure. Moreover, in the proposed approach, the latter security stage can be enhanced with new variants of ECDSA.

Another limitation of the proposed approach may be the lack of a "prize" for the completed PoW. This solution can be observed in cryptocurrency architectures. Without a "prize", the number of nodes that want to make the PoW may be insufficient to ensure a high level of security of the BIoMT network. Therefore, the author's research is focused on the use of TTP, where one of the selected nodes (e.g., a hospital) can play the role of TTP, especially since the data from the BIoMT network will contain medical records and will mostly be processed by devices and real-time hospital systems.

The proposed solution was implemented with the use of the MultiChain platform and experimentally verified. The created blockchain consists of 10k blocks; however, even with such a large number of blocks, the network functioned properly and efficiently. Future work of the authors will focus on the implementation of the blockchain with forks, Although this approach id rarely used, in the authors' opinion, it can be an interesting solution for some issues encountered in Blockchain implementations.

Author Contributions: Conceptualization, A.B. and G.B.; methodology, A.B.; validation, A.B. and K.K.; formal analysis, A.B., K.K., G.B. and R.W.; investigation, A.B.; resources, A.B.; data curation, A.B.; implementation, K.K.; expereminental verification, K.K. and G.B.; writing—original draft preparation, A.B., K.K., G.B. and R.W.; writing—review and editing, A.B., K.K., G.B. and R.W.; visualization, A.B.; supervision, A.B. and R.W.; project administration, A.B., G.B. and R.W.; funding acquisition, R.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Ministry of Education and Science, Poland, "Industrial doctorate", under the grant number DWD/4/90/2020.

Acknowledgments: This work is supported by the Ministry of Education and Science, Poland, "Industrial doctorate", under the grant number DWD/4/90/2020. The work is partially supported by Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, Andhra Pradesh, India. Figure 1 was prepared using pictures designed by macrovector/Freepik (http://www.freepik.com, accessed on 9 August 2022).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The appendix contains a script in Java language that was used in performance evaluation, as described in detail in Section 4.4. The script is responsible for the creation of 101 transactions for each type (one type stores data in a text form, the second in PDF format, and the last in graphical JPG format).

```
package ykarav.multichain;
import ykarav.multichain.chain.Chain;
import ykarav.multichain.chain.Method;
import ykarav.multichain.chain.MultichainService;
import java.io.*;
import java.nio.file.Files;
import java.nio.file.Paths;
import java.util.ArrayList;
import java.util.Collections;
import java.util.List;

public class TestApp extends Thread {
      public static void main(String[] args) throws IOException {

   //Configuration that we can connect to Blockchain
      Chain chain0 = Chain.initialize("192.168.96.106", 7762, "multichainrpc",
"J7Qm7UAeAbHWPJcYTUPfQPjC7c6QfKmsC1ApSVvowhBq", "BIoMT");
      MultichainService chainService = MultichainService.setChain(chain0);

   //From this address we send transactions
      String adress1 = "1YpnjLhP7yyYcakjRJmhjfCVLsFXDQb3buLsNp";

   //Declare parameters as params
      List<Object> params = null;

      params = new ArrayList<Object>();

   //Fill key list with data
      Object stream = new String("HPMS");
      ArrayList keys = new ArrayList();
      int block_type = 2;
      keys.add("block_type = " + block_type);
      String data_provider = "HPMS";
      keys.add("data_provider = " + data_provider);
      int data_reliability = 1;
      keys.add("data_reliability = " + data_reliability);
     int patient_ID = 1582;
      keys.add("patient_ID = " + patient_ID);
      Object options = new String();

   //Files used in tests
```

```
        String medicalFile132mb = "C:\\Users\\k.kozdroj\\Desktop\\nlst_test.csv";
        String pdfWithQSignature = "C:\\Users\\k.kozdroj\\Downloads\\blood_test.pdf";
        String rtg = "C:\\Users\\k.kozdroj\\Downloads\\radiology_test.jpg";

    //Convert the file to a binary table
        byte[] bytes = Files.readAllBytes(Paths.get(rtg));

    //Declare a new List for all transactions
        ArrayList<Double> allTransaction = new ArrayList<Double>();

    //Fill params with all necessary parameters
        Collections.addAll(params,adress1, stream, keys,bin2hex(bytes));

    //Get start time
        long startTime = System.nanoTime();

    //Declare loop for all transactions
   for(int counter = 0 ;counter <= 100; counter++)
   {
         long beforeTransaction = System.nanoTime();
         String jsonInString = chainService.apiCall(params, Method.PUBLISH_FROM,
chain0.getChainName());

    //Convert time to seconds
        double currentTime = (double) (System.nanoTime() - beforeTransaction)/1_000_000_000;

    //Add each transaction time to the List
        allTransaction.add(currentTime);
    }

   //Calculate the time of all transactions and print lists of each time transaction and full time
        long estimatedTime = System.nanoTime() - startTime;
        System.out.println(allTransaction);
        System.out.println(estimatedTime);
       double elapsedTimeInSecond = (double) estimatedTime/1_000_000_000;
        System.out.println(elapsedTimeInSecond + " seconds");
}

//This method convert binary table to hexadecimal format
public static String bin2hex(byte[] arr) {
        StringBuffer sb = new StringBuffer();

         for (int i = 0; i < arr.length; i++) {
             String str = Integer.toHexString((int) arr[i]);
             if (str.length() == 2)
                  sb.append(str);
             if (str.length() < 2) {
                  sb.append("0");
                  sb.append(str);
                  }
             if (str.length() > 2)
                  sb.append(str.substring(str.length() - 2));
             }
          return sb.toString();
          }
}
```

References

1. Fortune Business Insights, Internet of Medical Things (IoMT) Market, October 2021. Available online: https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844 (accessed on 26 June 2022).
2. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
3. Rodrigues, J.J.P.C.; Segundo, D.B.D.R.; Junqueira, H.A.; Sabino, M.H.; Prince, R.M.; Al-Muhtadi, J.; De Albuquerque, V.H.C. Enabling Technologies for the Internet of Health Things. *IEEE Access* **2018**, *6*, 13129–13141. [CrossRef]
4. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [CrossRef]
5. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
6. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. *IEEE Consum. Electron. Mag.* **2018**, *7*, 18–28. [CrossRef]
7. Zhang, J.; Xue, N.; Huang, X. A Secure System For Pervasive Social Network-Based Healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
8. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141. [CrossRef]
9. Bhattacharjya, A.; Zhong, X.; Li, X. A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme with Four-Layered Authentication Stack. *IEEE Access* **2019**, *7*, 30487–30506. [CrossRef]
10. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 131–143. [CrossRef]
11. More, S.; Chaudhari, S. Third Party Public Auditing Scheme for Cloud Storage. *Procedia Comput. Sci.* **2016**, *79*, 69–76. [CrossRef]
12. Li, C.-T.; Lee, C.-C.; Weng, C.-Y. A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System. *J. Med. Syst.* **2016**, *40*, 117. [CrossRef]
13. Lounis, A.; Hadjidj, A.; Bouabdallah, A.; Challal, Y. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Gener. Comput. Syst.* **2016**, *55*, 266–277. [CrossRef]
14. Kowalski, M.; Wiśniewski, R. Security Analysis of One-Time Pad Secure Algorithm Based on the Double Memory Technique, 2018. In Proceedings of the International Conference of Computational Methods in Sciences and Engineering-ICCMSE 2018, Thessaloniki, Greece, 14–18 March 2018; AIP Publishing: Melville, NY, USA, 2018. AIP Conference Proceedings. Volume 2040. [CrossRef]
15. Wiśniewski, R.; Grobelny, M.; Grobelna, I.; Bazydło, G. IoT Security with One-Time Pad Secure Algorithm Based on the Double Memory Technique, 2017. In Proceedings of the International Conference of Computational Methods in Sciences and Engineering-ICCMSE 2017, Thessaloniki, Greece, 21–25 April 2017; AIP Publishing: Melville, NY, USA, 2017. AIP Conference Proceedings. Volume 1906, ISBN 9780735415966. [CrossRef]
16. Di Pierro, M. What Is the Blockchain? *Comput. Sci. Eng.* **2017**, *19*, 92–95. [CrossRef]
17. Samaniego, M.; Jamsrandorj, U.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 433–436. [CrossRef]
18. Zubaydi, H.D.; Chong, Y.-W.; Ko, K.; Hanshi, S.M.; Karuppayah, S. A Review on the Role of Blockchain Technology in the Healthcare Domain. *Electronics* **2019**, *8*, 679. [CrossRef]
19. Viriyasitavat, W.; Xu, L.D.; Bi, Z.; Pungpapong, V. Blockchain and Internet of Things for Modern Business Process in Digital Economy—The State of the Art. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1420–1432. [CrossRef]
20. Johng, H.; Kim, D.; Hill, T.; Chung, L. Using Blockchain to Enhance the Trustworthiness of Business Processes: A Goal-Oriented Approach. In Proceedings of the 2018 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 2–7 July 2018; pp. 249–252. [CrossRef]
21. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1746–1761. [CrossRef]
22. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
23. Nakamoto, S. *Bitcoin: A Peer-To-Peer Electronic Cash System*; Decentralized Business Review; HN Publishing: Amsterdam, The Netherlands, 2008; p. 21260.
24. Zaman, U.; Imran; Mehmood, F.; Iqbal, N.; Kim, J.; Ibrahim, M. Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications. *Electronics* **2022**, *11*, 1893. [CrossRef]
25. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]

26. Khan, A.A.; Shaikh, Z.A.; Baitenova, L.; Mutaliyeva, L.; Moiseev, N.; Mikhaylov, A.; Laghari, A.A.; Idris, S.A.; Alshazly, H. QoS-Ledger: Smart Contracts and Metaheuristic for Secure Quality-of-Service and Cost-Efficient Scheduling of Medical-Data Processing. *Electronics* **2021**, *10*, 3083. [CrossRef]
27. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics* **2021**, *10*, 3003. [CrossRef]
28. Imran, M.; Zaman, U.; Imran; Imtiaz, J.; Fayaz, M.; Gwak, J. Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions. *Electronics* **2021**, *10*, 2501. [CrossRef]
29. Bazydło, G.; Wiśniewski, R.; Kozdrój, K. Trusted and Secure Blockchain-Based Durable Medium Electronic Service. *Cryptography* **2022**, *6*, 10. [CrossRef]
30. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR Mhealth Uhealth* **2017**, *5*, e111. [CrossRef]
31. Ahmad, L.; Khanji, S.; Iqbal, F.; Kamoun, F. 2020. Blockchain-based chain of custody: Towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20), Dublin, Ireland, 25–28 August 2020; Association for Computing Machinery: New York, NY, USA, 2020. Article 48. pp. 1–8. [CrossRef]
32. Nayak, A.; Dutta, K. Blockchain: The perfect data protection tool. In Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 23–24 June 2017; pp. 1–3. [CrossRef]
33. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
34. Wang, Z.; Lin, J.; Cai, Q.; Wang, Q.; Zha, D.; Jing, J. Blockchain-Based Certificate Transparency and Revocation Transparency. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 681–697. [CrossRef]
35. Abe, R.; Watanabe, H.; Ohashi, S.; Fujimura, S.; Nakadaira, A. Storage Protocol for Securing Blockchain Transparency. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; pp. 577–581. [CrossRef]
36. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Security Challenges and Concerns of Internet of Things (IoT). In *Cyber-Physical Systems: Architecture, Security and Application, EAI/Springer Innovations in Communication and Computing*; Guo, S., Zeng, D., Eds.; Springer: Cham, Switzerland, 2018; pp. 153–185. [CrossRef]
37. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Secure IoT Structural Design for Smart Homes, Chapter 13. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 187–201. ISBN 9780128150320. [CrossRef]
38. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Present Scenarios of IoT Projects with Security Aspects Focused. In *Digital Twin Technologies and Smart Cities. Internet of Things*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2020. [CrossRef]
39. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. CoAP—Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In *Digital Twin Technologies and Smart Cities*; Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Internet of Things; Springer: Cham, Switzerland, 2020. [CrossRef]
40. Wiśniewski, R.; Wiśniewski, R. Representation of Primes in the Form p = 6 " x=1 and its Application to the RSA Prime Factorization, 2018. In Proceedings of the International Conference of Computational Methods in Sciences and Engineering-ICCMSE 2018, Thessaloniki, Greece, 14–18 March 2018; AIP Publishing: New York, NY, USA, 2018. AIP Conference Proceedings. Volume 2040. [CrossRef]
41. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
42. Ekparinya, P.; Gramoli, V.; Jourjon, G. Impact of Man-In-The-Middle Attacks on Ethereum. In Proceedings of the 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS), Salvador, Brazil, 2–5 October 2018; pp. 11–20. [CrossRef]
43. Vanstone, S.A. Responses to NIST's proposal. *Commun. ACM* **1992**, *35*, 41–54. [CrossRef]
44. Long, T.; Liu, X. Two Improvements to Digital Signature Scheme Based on the Elliptic Curve Cryptosystem. In Proceedings of the International Workshop on Information Security and Application (IWISA 2009), Toyama, Japan, 25–27 August 2009; Academy Publisher: Bengaluru, India, 2009.
45. Bi, W.; Jia, X.; Zheng, M. A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain. *arXiv* **2018**. [CrossRef]
46. Cano, M.; Cañavate-Sanchez, A. Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA. *Secur. Commun. Netw.* **2020**, *2020*, 4960964. [CrossRef]
47. Salim, M.M.; Kim, I.; Doniyor, U.; Lee, C.; Park, J.H. Homomorphic Encryption Based Privacy-Preservation for IoMT. *Appl. Sci.* **2021**, *11*, 8757. [CrossRef]
48. Blake, I.; Seroussi, G.; Smart, N.P. *Advances in Elliptic Curve Cryptography*; London Mathematical Society Lecture Note Series; Cambridge University Press: Cambridge, UK, 2005. [CrossRef]
49. Bekyel, E. The density of elliptic curves having a global minimal Weierstrass equation. *J. Number Theory* **2004**, *109*, 41–58. [CrossRef]
50. Hankerson, D.; Menezes, A. Elliptic Curve Discrete Logarithm Problem. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011. [CrossRef]
51. Caelli, W.J.; Dawson, E.P.; Rea, S.A. PKI, elliptic curve cryptography, and digital signatures. *Comput. Secur.* **1999**, *18*, 47–66. [CrossRef]

52. Radoglou-Grammatikis, P.; Rompolos, K.; Sarigiannidis, P.; Argyriou, V.; Lagkas, T.; Sarigiannidis, A.; Goudos, S.K.; Wan, S. Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2041–2052. [CrossRef]
53. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access* **2019**, *7*, 74361–74382. [CrossRef]
54. MultiChain Project Website. Available online: https://www.multichain.com/ (accessed on 26 June 2022).
55. National Lung Screening Trial (Cancer Imaging Archive) Website. Available online: https://wiki.cancerimagingarchive.net/display/NLST/ (accessed on 9 August 2022).
56. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
57. Croman, K.; Eyal, I. On Scaling Decentralized Blockchains (PDF). Financial Cryptography and Data Security. *Lect. Notes Comput. Sci.* **2016**, *9604*, 106–125. [CrossRef]
58. IPFS Project Website. Available online: https://ipfs.tech/ (accessed on 9 August 2022).