electronics

MDPI

Review

A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain

Fariza Sabrina [1,*,†], Shaleeza Sohail [2,†] and Umair Ullah Tariq [1]

[1] School of Engineering and Technology, Central Queensland University, Rockhampton, QLD 4701, Australia; u.tariq@cqu.edu.au
[2] College of Engineering, Science and Environment, The University of Newcastle, Callaghan, NSW 2308, Australia; shaleeza.sohail@newcastle.edu.au
* Correspondence: f.sabrina@cqu.edu.au
† These authors contributed equally to this work.

Abstract: The Internet of Medical Things (IoMT) has significantly enhanced the healthcare system by enabling advanced patient monitoring, data analytics, and remote interactions. Given that IoMT devices generate vast amounts of sensitive data, robust privacy mechanisms are essential. This privacy requirement is critical for IoMT as, generally, these devices are very resource-constrained with limited storage, computation, and communication capabilities. Blockchain technology, with its decentralisation, transparency, and immutability, offers a promising solution for improving IoMT data security and privacy. However, the recent emergence of quantum computing necessitates developing measures to maintain the security and integrity of these data against emerging quantum threats. This work addresses the current gap of a comprehensive review and analysis of the research efforts to secure IoMT data using blockchain in the quantum era. We discuss the importance of blockchain for IoMT privacy and analyse the impact of quantum computing on blockchain to justify the need for these works. We also provide a comprehensive review of the existing literature on quantum-resistant techniques for effective blockchain solutions in IoMT applications. From our detailed review, we present challenges and future opportunities for blockchain technology in this domain.

Keywords: quantum computing; privacy preservation; blockchain; IoMT; post-quantum

Citation: Sabrina, F.; Sohail, S.; Tariq, U.U. A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain. *Electronics* **2024**, *13*, 2962. https://doi.org/10.3390/electronics13152962

Academic Editors: Abdussalam Elhanashi and Pierpaolo Dini

Received: 31 May 2024
Revised: 19 July 2024
Accepted: 22 July 2024
Published: 26 July 2024

1. Introduction

The Internet of Things (IoT) has significantly improved various aspects of our daily lives. However, these devices are vulnerable to security threats due to its resource-constrained nature. Several research efforts have provided security solutions for IoT devices using contemporary and emerging technologies [1]. IoT has a huge impact on the health domain and the rapid evolution of IoMT has enabled unprecedented levels of patient monitoring, data analytics, and remote medical interactions. As these technologies integrate more deeply into healthcare infrastructures, they generate vast amounts of sensitive medical data, necessitating robust privacy preservation mechanisms. Some of the common techniques to secure IoMT-generated sensitive medical data are cryptographic algorithms, access control mechanisms, machine learning approaches, blockchain, and steganography [2]. The advent of quantum computing provides access to new and emerging quantum-enabled security solutions for the healthcare domain [3]. However, it also poses new challenges to the existing security measures, threatening the integrity and confidentiality of IoMT data. These emerging threats require the development of post-quantum solutions to safeguard medical data against future quantum-enabled attacks [4].

One of the recent technologies used for enhancing data security for IoT-based applications is Blockchain due to its decentralisation, transparency, and immutability. For healthcare IoMT applications, this technology is a promising option for enhancing data security and privacy. One of the main strengths is that by leveraging blockchain, it is

possible to create a secure and transparent environment for managing IoMT health data, where modifications are traceable and immutable, which makes it very attractive for applications with sensitive data. Additionally, blockchain can facilitate secure, decentralised data exchanges across the network without relying on trusted third parties, thus reducing vulnerability points for healthcare applications. Hence, we only consider blockchain-based security solutions for healthcare IoMT applications in this work.

Recently, quantum computing has emerged as a critical technology with an immense amount of computing power that helps solve problems that cannot be solved by classical computers [5]. However, in addition to the huge benefits that can be provided by this technology some threats to existing techniques are posed as well. A common concern in this area is the vulnerability of existing cryptographic algorithms to the quantum era. Most of these cryptographic algorithms rely on the fact that they cannot be solved by classical computers due to limited computing resources; however, quantum speed-up will break this barrier by making a huge amount of computing power available for decrypting these algorithms.

The rest of the paper is organised as follows. Section 2 discusses the importance of blockchain technology for IoMT privacy preservation. Section 3 discusses the key algorithms in post-quantum cryptography and compares those algorithms based on their strength and utilisation. Section 4 analyses how blockchain technology is affected by quantum computing due to its reliance on cryptographic algorithms. Section 5 provides a performance comparison of post-quantum cryptographic algorithms for IoT devices. in Section 6, we provide a comprehensive review of the existing literature addressing quantum-resistant techniques for effective blockchain solutions for IoMT applications. Section 7 summarises the key approaches against quantum attacks discussed in this paper and future research opportunities in this domain, and Section 8 concludes our paper.

2. Background

In this section, we will briefly look at the emerging use of IoMT in healthcare applications and emphasise the importance of privacy preservation requirements for these applications due to the inherent constraints associated with these devices. We will review some of the common techniques used for providing data privacy for these applications. The last subsection focuses on discussing the architecture and mechanism of blockchain technology that make it suitable for this purpose. With recent advancements in quantum computing, all these blockchain-based approaches can become vulnerable and will not be able to resist quantum attacks. Hence, in this paper, we will analyse all the existing research efforts in the field of post-quantum cryptography that can provide privacy for blockchain solutions for healthcare IoMT applications.

2.1. Overview of Internet of Medical Things

The Internet of Medical Things can be defined as a network comprising medical devices and individuals, utilising wireless communication to facilitate the exchange of healthcare information [6]. IoMT enables the seamless collection, analysis, and transmission of health data, empowering healthcare providers to make better decisions, monitor patients more effectively, and provide personalised care remotely [7]. Ultimately it enhances healthcare delivery by making it more efficient, cost-effective, and patient-centric.

Key aspects of IoMT include its ability to connect various medical devices and sensors that monitor vital patient data in real time. These devices can communicate and share information over the Internet, allowing for immediate medical interventions and continuous patient monitoring without the need for physical presence. This technology is particularly beneficial in managing chronic diseases, improving emergency responses, and optimising hospital operations by reducing unnecessary visits and streamlining processes [7].

Irrespective of the transformative benefit that IoMT brings to healthcare applications, it presents several significant challenges in terms of privacy, security, heterogeneity, interoperability, the availability of data, etc. IoMT devices come with diverse specifications in

terms of hardware and software (such as connections, power requirements, processing capabilities, supported protocols, and security measures), and this heterogeneity among the devices which can be part of one network elevates the system's susceptibility cyber attacks. Hence, the use and integration of IoMT devices into healthcare systems present both a technical challenge and a critical opportunity for improving patients' experience [8].

2.2. Importance of Privacy Preservation for IoMT

Privacy preservation refers to the techniques and methods used to protect sensitive and private information from unauthorised access, disclosure, or misuse while maintaining the functionality and quality of service of the application [9]. Privacy preservation in medical data is crucial due to the highly sensitive nature of personal health information. Unauthorised access can lead to significant privacy violations and misuse of data, including identity theft and discrimination. Medical data often include not only health information but also personally identifiable information, which, if exposed, can harm the patient's privacy and security. Additionally, the potential for cyber attacks on healthcare systems necessitates robust security measures to protect these data from being compromised.

IoMT devices collect highly sensitive health and medical data, including medical histories, current health status, and biometric information. Ensuring the privacy of these data from unauthorised access is essential to maintain patient privacy and trust in healthcare applications [10].

2.3. Privacy Preservation Techniques for IoMT

A significant amount of work has been conducted in the existing literature highlighting the technologies that could protect the privacy of medical data. Some of the technologies that could be used to ensure privacy in IoMT are as follows:

- Cryptographic Algorithms: Cryptographic algorithms include methods that are used to secure and protect data and communication by applying complex mathematical and logical techniques. Data encryption is one of the principal applications of cryptography that ensures the data are encrypted at their sources and decrypted only at their destination, and hence it prevents unauthorised access during the transmission of data. Homomorphic encryption and secret sharing ensure that even when data are processed or analysed by third-party systems, the privacy and integrity of the data remain intact, preventing any unauthorised access or interpretation of sensitive information [11].
  Putra et al. [12] highlight that centralised medical data repositories, while useful for streamlined data access and efficient healthcare workflows, are vulnerable to security threats such as unauthorised access and cyber attacks. These threats jeopardize the integrity and confidentiality of sensitive patient information. To mitigate these risks, the authors emphasise the necessity of robust security measures, including encryption, access control, and breach detection mechanisms.
- Anonymisation and Pseudonymisation: Anonymisation removes personally identifiable information, making data untraceable to individuals. Pseudonymisation replaces private data identifiers with artificial identifiers or pseudonyms, protecting privacy while allowing data analysis without directly exposing personal information [13].
- Privacy-Preserving Machine Learning: Machine learning has been one of the most used approaches when it comes to data privacy preservation in any domain [14]. Different machine learning approaches like SVM, CNN, deep learning, and multiple ensemble approaches have been used for the detection and mitigation of security and privacy attacks when IoT devices are used [15]. Distributed machine learning approaches like federated learning allow model training on multiple devices with local data, which eliminates the requirement of exchanging data and, hence, minimises privacy concerns [16]. To further mitigate privacy attacks, Differential Privacy can be utilised, which adds noise to the data or to the outputs of data analyses to obscure the presence or absence of individuals in the data set [17].

- Edge Computing: Processing data at the edge (closer to where they are generated) reduces the need to transmit sensitive information over the network, thus enhancing privacy. As mentioned in [12], cloud-edge computing, federated learning, and AI could secure and preserve the privacy of medical data in the IoMT ecosystem.
- Blockchain: Blockchain can significantly enhance privacy preservation in medical data through its decentralised architecture, which eliminates the need for a central authority, reducing the risk of data tampering and unauthorised access. Each transaction on the blockchain is encrypted and linked to the previous one, creating an immutable ledger. This ensures that medical records are secure and can only be accessed by parties who have been granted permission, enhancing patient privacy. Furthermore, the use of smart contracts on blockchain platforms can automate the consent management process, allowing patients to control who can access their data and for what purpose, ensuring compliance with privacy regulations like HIPAA. Additionally, blockchain's transparency feature can be fine-tuned to balance confidentiality with the traceability of access and changes to data, making it a robust solution for securing sensitive health information [18]. For example, [19] proposed quantum blockchain technology called the Quantum Blockchain Integrated Medical Data Processing System (QB-IMD), providing a promising solution to these emerging threats. The QB-IMD system utilises a quantum blockchain structure along with a novel Electronic Medical Record Algorithm (QEMR) to ensure data legitimacy and tamper-proofing through quantum signatures and quantum identity authentication. Elkhodr et al. [20] proposed a blockchain-based framework aimed at secure and privacy-preserving biomedical data sharing. The authors demonstrated that the proposed blockchain-based solution is efficient in enhancing the privacy of data in the sharing of biomedical data.
- Hybrid Approaches: A combination of blockchain technology and federated learning (FL) can also be employed to efficiently tackle privacy issues in IoMT [21]. Ali et al. [22] present a framework that integrates deep learning, homomorphic encryption, and blockchain to enhance the privacy and security of medical data. The consortium blockchain component provides a decentralised and immutable ledger to manage data access, ensuring that only authorised parties can access sensitive information. Smart contracts within the blockchain enforce access control policies, maintaining data integrity and preventing unauthorised access. Together, these technologies create a robust solution for the secure, efficient, and privacy-preserving management of medical data in the Industrial Internet of Medical Things (IIoMT).

Among the above-mentioned approaches, end-to-end encryption is often considered the most foundational and effective for the immediate protection of data in transit and at rest. For comprehensive privacy preservation, combining multiple technologies such as encryption with blockchain for secure data management and federated learning for privacy-preserving analytics can provide a robust solution. However, hybrid approaches come with their challenges and limitations and the integration of these approaches is non-trivial in most application architectures. In this paper, we only consider the use of blockchain for privacy preservation in IoMT-based applications. In the next section, we first look at the workings of blockchain and then further elaborate on how quantum computing can affect this technology and related healthcare applications.

2.4. Overview of Blockchain

Blockchain is a decentralised and distributed digital ledger technology that records transactions across multiple nodes in a peer-to-peer network [23]. In blockchain, once a record is made, it cannot be altered. The structure of blockchain consists of data blocks that are sequentially linked, creating a continuously growing chain as new transactions are recorded. Each block confirms the timing and sequence of transactions, securely maintained within a network that operates under mutually agreed-upon rules. Key characteristics of blockchain include the following:

1. Decentralisation:Data are spread across a network of computers rather than being stored in a central database, reducing dependency on any single authority and enhancing security.
2. Transparency: All transactions are visible to network participants, ensuring that any data recorded are easily verifiable and auditable, fostering trust among users.
3. Immutability: Once data are entered into the blockchain, it is nearly impossible to modify them, ensuring data integrity.
4. Security: Advanced cryptographic techniques protect data, preventing unauthorised access and ensuring that each transaction is securely linked to the previous one.

2.5. Blockchain and IoMT Integration

In healthcare, blockchain's significant potential lies in its ability to revolutionise medical data management and patient care [24]. It can enhance how medical information is shared and managed among various stakeholders, including hospitals, doctors, and insurance companies. By offering a secure and transparent environment, blockchain ensures that medical records are not only protected against unauthorised access but are also immutable and traceable. This can lead to improved treatment structures and more coordinated patient care based on a globally accessible system.

Overall, blockchain can play a crucial role in healthcare, offering robust solutions for secure data storage, the efficient exchange of patient records, and a foundation for various other applications. This technology not only promises to safeguard sensitive information but also to significantly improve operational efficiencies and patient outcomes in the healthcare sector.

Cryptography is one of the main components of security in blockchain technology;' it is pivotal for ensuring the technology's reliability and trustworthiness while preserving data integrity [25]. By employing cryptographic methods, sensitive information like identity verification and financial transactions remains protected, fostering trust among users and reinforcing the security of blockchain networks. Public-key or asymmetric cryptography is essential for securely engaging with the blockchain, enabling the verification of transactions. Additionally, hash functions play a crucial role by facilitating the creation of digital signatures and linking blocks. Despite their importance, both public-key cryptosystems and hash functions are vulnerable to potential threats posed by the advancement of quantum computing technology, which could compromise the security of blockchain systems in the future [26].

3. Post-Quantum Cryptography

Quantum computing can provide a wealth of solutions for problems that have been unsolvable using traditional computing methods. One branch of that would be to use quantum physics for securing communication, known as quantum cryptography. However, the existing cryptographic techniques and algorithms were designed considering the infeasibility of finding mathematical solutions using traditional computing and these will not be effective against quantum computing. Hence, researchers have been redesigning cryptographic algorithms that can be used to protect communication and data after quantum computers are more readily available [5].

Quantum computing exploits the vulnerabilities of traditional cryptographic algorithms and makes them obsolete for securing data or communication purposes. Public-key cryptography is severely affected by quantum speed-up of factoring large numbers, which significantly reduces the time required to break these algorithms. Similarly, symmetric encryption faces the challenge of severely reduced strength due to quantum speed-up [27].

Post-quantum cryptography (PQC) focuses on developing cryptographic algorithms based on mathematical problems that are resistant to traditional and quantum computing. Some of the most prominent approaches in this field are briefly discussed below and are compared in Table 1 [28]:

- Lattice-based cryptography [29];

- Hash-based cryptography [30];
- Code-based cryptography [31];
- Multivariate polynomial cryptography [32].

Table 1. Comparison of post-quantum cryptographic approaches.

	Lattice-Based Cryptography	**Hash-Based Cryptography**	**Code-Based Cryptography**	**Multivariate Polynomial Cryptography**
Technique	Hard lattice problems	Hash functions	Error correction codes	Solving polynomial equations
Applications	Key exchange encryption	Digital signature	Key exchange encryption	Digital signature encryption
Strength	Hardness of lattice problems	Well-tested hash-based security	Proven security in decoding	Effective verification
Issues	Large key size, complex lattice -based maths	Large key size, large signature, non-versatile	Large key size, efficiency	Large key size, key generation
Implemented Algorithms	KYBER SABER	SPHINCS+ XMSS	McEliece BIKE	Rainbow GeMSS

A fundamental block of lattice-based cryptography is a lattice, a mathematical structure in a multi-dimensional space that is composed of a repeating grid generated by a periodic repeat of a unit cell across all dimensions. A lattice is a linear combination of basis vectors and the selection of these basis vectors defines the geometry of a lattice. The fact that a lattice is a multi-dimensional repeating structure with geometry depending upon the basis vectors provides an immense number of configurations, which is a required feature of a cryptographic technique. The geometric and computational complexity involved in solving lattice problems, which consist of certain operations in lattice structures and increase with the increase in lattice dimensions, makes these problems intractable for quantum and traditional computing. Lattice problems are quantum-resistant as there is no known algorithm capable of solving them due to their high-dimensional nature [29].

Hash-based cryptography employs a deterministic, computationally quick, pre-image and collision-resistant hash function with an avalanche effect. Some quantum algorithms may be able to find collisions in these hash functions; however, with large hash sizes, hash-based cryptography may still be quantum-resistant depending upon the size of the hash [30].

Code-based cryptography relies on Error Correcting Codes (ECCs) by adding redundant bits in data to detect and correct errors. Some of the main approaches in this area rely on difficult decoding of the randomly generated linear code. The inability of quantum algorithms to decode random linear code makes this a suitable candidate for post-quantum cryptography [31].

Multivariate polynomial cryptography is based on systems of polynomial equations involving mathematical operations and multiple variables. The computational difficulty associated with the solution of these equations in high-dimensional space makes these cryptographic schemes quantum-resistant [32].

The above-mentioned cryptographic approaches are quantum-resistant and may provide data and communication security and privacy in the post-quantum era. However, every approach has its limitations and challenges that reduce its applicability in practical scenarios. The focus of this work is to analyse the post-quantum cryptographic approaches

that are necessary for the secure and optimal function of blockchain-based privacy solutions in IoMT [33].

The research, development, and standardisation of cryptographic algorithms that are quantum-resistant is an ongoing effort by the National Institute of Standards and Technology (NIST) [34]. This is a rapidly changing area of research and development where, recently, four primary quantum-resistant algorithms were selected for testing and standardisation to withstand potential threats by quantum machines.

4. Blockchains and Quantum Computing

The emergence of quantum computing in recent years requires safeguarding some of the fundamental building blocks of blockchain technology. As discussed in the previous section, in the post-quantum era cryptographic algorithms such as public key and hash-based ones may come under threat. In light of these issues, researchers in the blockchain field have started looking into finding solutions that are quantum-resistant. The first set of solutions is called post-quantum blockchain and relies on using post-quantum encryption methods for securing blockchains. The second set of approaches, known as quantum blockchain, utilises quantum computers and networks to redesign blockchain structure [35]. The focus of this paper is post-quantum blockchain techniques to secure blockchains in the quantum era.

Let us first look at the challenges faced by blockchain technology in quantum computing that can disrupt its normal working. Two quantum algorithms can play a big part in this disruption, which are briefly discussed in the following subsections:

- Shor's algorithm [36];
- Grover's algorithm [37].

4.1. Shor's Algorithm

Shor's algorithm is one of the most important developments for quantum technology as it not only factorises large numbers efficiently but also has an associated practical problem for which quantum speed-up can play a significant part. Shor's factorisation algorithm finds the prime factors of any number by using modular arithmetic. In modular arithmetic, a period is defined as the number of steps that take us back to the start of a loop. The period of $amoduloN$ can provide prime factors of N in a limited number of tries. A number of steps are involved in this process and all of those can be processed effectively on a classical computer but one, which can be extremely computationally intensive. However, quantum computers can process that step with great efficiency and hence can find the prime factors of a very large number in logarithmic time [36].

One of the most used asymmetrical cartographic algorithms is the Rivest–Shamir–Adleman (RSA) algorithm, which uses public and private key pairs for the encryption and decryption of data [38]. When any data are encrypted using a public key, then they can only be decrypted using a corresponding private key. The public and private key pair is generated using a mathematical algorithm while considering a large number and its factors. If a public key is known, then finding a corresponding private key is not a trivial task. This cryptosystem is considered safe as factorisation of a considerably large number is a very difficult problem for classical computers. However, while using quantum computing, Shor's factorisation algorithm can find these factors in a very short time and, hence, can generate the private key that makes these cryptosystems vulnerable and not usable.

4.2. Grover's Algorithm

Grover's quantum algorithm is a search algorithm that can search unstructured data with quadratic improvement as compared to classical search algorithms. One of the main ideas behind Grover's algorithm is the use of a diffusion operator that amplifies the amplitude of the value that is being searched by the searching algorithm and hence increases the probability of finding that value among all possible values in unstructured

data. By performing this amplification almost $\sqrt{n}$ number of times, the amplitude of the searched value will be almost one and the result can be measured [37].

Hash-based cryptography uses a mathematical function to convert a variable length input to a fixed length output. The main properties of these algorithms that make them suitable for encrypting data are that from a given output it is difficult to guess input and, secondly, there is a very low probability that any two inputs will give the same output (hash collision). A method for finding hash collision requires searching an entire search space, which is currently computationally infeasible using classical computers. Grover's quantum algorithm can search in time of order $O(\sqrt{n})$, which may result in compromised hash when using quantum computers.

4.3. Effect of Quantum Algorithms on Blockchain Security and Functioning

In a blockchain network, an address is given to every user as a unique identifier for carrying out transactions. These blockchain addresses require public-key cryptography to generate public and private key pairs. The public key is available for everyone and the user securely holds the private key. The user uses a private key to sign transactions that can be authenticated by anyone in the network with a public key to ensure that the transaction is signed by the correct user. By using a hashing function on the user's public key, a user-friendly blockchain address is created which is used for any transactions. The guarantee of authenticity for transactions signed by the user's private key is based on the assumption that the publicly available key cannot be used to regenerate the corresponding private key due to the factorisation difficulty faced by these classical computers [35].

Some of the most popular blockchain implementations use RSA and similar approaches based on factorisation difficulty assumption. The quantum speed-up with Shor's algorithm for factorisation can break such asymmetric key algorithms even when using a 2048 bit number in only a few minutes as compared to the millions of years of computing time required for this using classical computers. A quantum user can regenerate the private keys from the public keys of all other users and can start fraudulent transactions on behalf of any other user.

Blocks in blockchain networks store transactions and hash values of the previous block in order to connect to a previous block in a chain pattern. Any change to any block in the chain will break the chain if hashes for all preceding blocks are not recalculated. SHA256 [39] is a commonly used hash function to calculate hashes for blocks that are used to point to a previous block in the chain.

As previously discussed, these hash functions exhibit the non-reversible property that from the hash the input data cannot be regenerated. However, the other important property of hash functions is collision resistance which can be exploited using Grover's quantum algorithm by recreating subsequent blocks in the blockchain compromising the main strength of the blockchain, which is immutability. Furthermore, quantum miners may have an advantage as compared to miners using classical computers when it comes to proof of work census algorithms. For this algorithm, brute force searching is used to find a hash that meets specific requirements, and with quantum speed-up that may become easier for some users.

5. Post-Quantum Cryptography in Resource-Constrained Devices

The performance comparison of post-quantum cryptographic algorithms in several IoT devices highlights the importance of evaluating both Key Encapsulation Mechanisms (KEMs) and digital signatures. IoT devices, often constrained by limited computational power and memory, require cryptographic solutions that are both secure and efficient. This discussion addresses how different algorithms perform on IoT devices, focusing on KEMs and digital signature schemes.

Table 2 highlights the performance of various post-quantum cryptographic algorithms in several IoT devices, specifically addressing the concerns of resource constraints. The following are the key takeaways:

1. **Key Encapsulation Mechanisms (KEMs):** KEM algorithms are essential for securely exchanging keys between devices in an IoT network, particularly where resources are limited. The study by Halak et al. [40] demonstrated that both Kyber and SABER are efficient in terms of code size and RAM usage on ARM Cortex-M3 and Cortex-M0 devices, making them suitable for resource-constrained environments. Tasopoulos et al. [41] found that Kyber offers the best overall performance on ARM Cortex-M4 devices, while SIKE has the smallest public key and ciphertext sizes but slower execution times. Satrya et al. [42] highlighted that NTRU outperforms SABER and RSA in CPU and memory usage on Raspberry Pi-4, with Light SABER showing the best encryption/decryption delays. Mohamed et al. [43] confirmed that Kyber512 is efficient in key encapsulation and decapsulation times on a Kubernetes-managed Raspberry Pi 4 cluster, which is suitable for time-sensitive medical applications.
2. **Digital Signatures:** Digital signatures are crucial for verifying the authenticity and integrity of messages in IoT networks. Halak et al. [40] indicated that FALCON, with its low latency, is suitable for applications requiring fast verification on ARM Cortex-M3 and Cortex-M0 devices. Tasopoulos et al. [41] observed that Dilithium offers the most balanced performance on ARM Cortex-M4, while Falcon outperforms RSA at security level 1. Vidakovic et al. [44] corroborated these findings across ARM Cortex-M4, x86/x64 processors, and FPGA, noting that Dilithium provides balanced performance and Falcon excels in all operations at security level 1.

Table 2. Performance comparison of post-quantum cryptography algorithms in several IoT devices.

Ref.	Hardware	Software Library	Type	Candidates	Criteria	Result
Halak et al. [40]	ARM Cortex-M3, ARM Cortex-M0	Mbed TLS	KEM	Kyber, SABER	Code-size/RAM	Kyber, SABER
			Signature	Dilithium, FALCON	Code-size/Latency	FALCON
Tasopoulos et al. [41]	ARM Cortex-M4	wolfSSL	KEM	SABER, NTRU, SIKE, BIKE, HQC, NTRU LPRime, FrodoKEM	Execution Speed, Memory Requirements, Communication Size	Kyber offers the best overall performance; SIKE has the smallest public key and ciphertext sizes but the slowest execution time
			Signature	Dilithium, Falcon, SPHINCS+, Picnic3	Execution Speed, Memory Requirements, Communication Size	Dilithium offers the most balanced performance; Falcon outperforms RSA in all operations at security level 1
Vidakovic et al. [44]	ARM Cortex-M4, x86/x64 processors, FPGA	Not given	KEM	Not covered	Not applicable	Not applicable
			Signature	Dilithium, Falcon, SPHINCS+, Picnic3	Execution Speed, Memory Requirements, Communication Size	Dilithium offers the most balanced performance; Falcon outperforms RSA in all operations at security level 1
Mohamed et al. [43]	Raspberry Pi-4 (RPi-4)	Custom implementations for RSA, NTRU, and SABER	KEM	RSA, NTRU, SABER (including Light SABER)	CPU Usage, RAM Usage, Encryption/Decryption Time	NTRU outperforms SABER and RSA in terms of CPU and memory usage; Encryption/Decryption Time: Light SABER is the front-runner when considering encryption and decryption delays
			Signature	Not covered	Not applicable	Not applicable
Satrya et al. [42]	Raspberry Pi 4, Cluster HAT with Raspberry Pi Zero	Kubernetes (K3S) and Docker	KEM	CRYSTAL-Kyber	CPU Usage, Memory Usage, Encryption/Decryption Time, Scalability and Performance Metrics	Kyber512 demonstrated efficient key encapsulation and decapsulation times
			Lightweight Cryptography	ASCON	CPU Usage, Memory Usage, Encryption/Decryption Time, Scalability and Performance Metrics	ASCON showed effective encryption and decryption times suitable for time-sensitive medical applications

In conclusion, for resource-constrained IoT devices, lightweight cryptographic algorithms like ASCON are crucial due to their efficient CPU and memory usage. Post-quantum algorithms like CRYSTAL-Kyber, while providing robust security, need optimization to be feasible in such environments. The studies show that optimized post-quantum algorithms can offer both security and efficiency. Nevertheless, it can generally be concluded that post-quantum cryptographic schemes can be implemented and operated on current limited-resource devices in different IoT applications [45]. Furthermore, it can be observed that lattice-based schemes perform better than other types in terms of speed, memory, and energy consumption. A hybrid approach combining lightweight and post-quantum cryptography may provide the best balance for securing IoT devices without compromising performance.

6. Existing Work

In this section, first we discuss some of the research contributions targeting post-quantum IoMT privacy preservation. After that, we discuss research efforts that specifically target post-quantum blockchain-assisted privacy preservation for IoMT. In the last subsection, we briefly describe how quantum blockchain provides security and privacy for IoMT applications.

6.1. Privacy Preservation for Post-Quantum IoMT

Current privacy preservation methods are insufficient against quantum attacks and often come with high computational overheads [46]. By incorporating lattice-based cryptography, which is believed to be resistant to quantum decryption methods, these gaps could be addressed. Chen et al. [46] propose a scheme that utilises hash operations and error reconciliation technology to provide highly secure and flexible authentication suitable for the cloud environment

Li et al. [47] proposed the Healthchain system, which focuses on the privacy-preserving sharing of electronic medical records (EMRs) using a group signature scheme (GSS). The Healthchain system employs blockchain technology to avoid data tampering and ensures the privacy and security of user data. The system uses an EMR group verification model where EMR data are verified by a creating group to form a transaction and transaction data are verified by system-maintaining nodes to achieve network consensus. The incorporation of a lattice-based GSS strengthens the quantum security of the EMR verification model, providing secure verification, anonymity, traceability, and non-frameability. This scheme supports group members with free joining and revoking, making it a robust solution for EMR management in the IoMT environment.

Yadav et al. [48] focus on designing a privacy-preserving authenticated key mechanism for IoMT systems. The proposed protocol utilises the "ring learning with errors" (RLWE) assumption and physical unclonable functions (PUFs) to achieve robust security. The RLWE-based protocol ensures that the authentication and key exchange mechanisms are secure against quantum attacks. The use of PUFs adds a layer of security by leveraging the unique physical characteristics of devices, making them difficult to clone or forge. This combination of advanced cryptographic techniques provides a high level of security and privacy for IoMT data, protecting them from classical and quantum threats.

6.2. Post-Quantum Blockchain-Assisted Privacy Preservation for IoMT

Shuaib et al. [49] discussed the significant impact of quantum computing on the security and reliability of blockchain-based EHR systems. Quantum computing poses a substantial threat to the traditional cryptographic methods used in blockchain due to its ability to solve complex mathematical problems quickly. The paper highlights the necessity of transitioning to quantum-resistant cryptographic algorithms to safeguard EHR systems against quantum attacks. It emphasizes the importance of post-quantum cryptographic solutions, such as lattice-based cryptography, to ensure the continued security and integrity

of blockchain-based healthcare data management systems in the face of emerging quantum computing capabilities.

liu et al. [50] presented a lattice-based proxy-oriented public auditing scheme for electronic health records in cloud-assisted Wireless Body Area Networks (WBANs). The proposed scheme utilises identity-based cryptography to avoid complex certificate management and introduces a proxy to handle signature generation, significantly reducing the computational burden on resource-constrained mobile devices. Additionally, the scheme incorporates Ethereum blockchain technology to protect against malicious proxies. The approach ensures security against quantum attacks, proxy protection, unforgeability, and privacy preservation.

Zhao et al. [51] present an advanced approach for securing IoT in smart healthcare. The Brooks Iyengar quantum Byzantine Agreement-centred blockchain Networking (BIQBA-BCN) model ensures the sincerity and equity of health data exchange. It uses a mutual authentication system based on the Blum Blum Shub and Okamoto Uchiyana Cryptosystem (BBS-OUC) and a Key Weight Block Function-Quasi-Cyclic Moderate Density Parity Check (KWBF-QCMDPC) algorithm to safeguard the confidentiality and dependability of IoT user data. The BBS-OUC cryptosystem leverages the complexity of prime factorisation and discrete logarithms, making it resistant to quantum computing threats. The KWBF-QCMDPC algorithm further enhances security by providing error-correcting codes that are difficult for quantum computers to break. This combination of advanced cryptographic techniques ensures that the BIQBA-BCN model is highly effective against quantum attacks. It has been claimed that the model provides high security and scalability, achieving a security level of 94% and offering significant improvements in data throughput, consensus latency, and node communication time.

A consortium blockchain framework for securing electronic health records (EHRs) using post-quantum cryptography is proposed [52] that employs the CRYSTALS Kyber-768 public key cryptosystem to provide security against quantum attacks. This system ensures data security, confidentiality, and integrity while giving individuals absolute authority over their health data. By using lattice-based cryptography, which relies on the hardness of problems like Learning with Errors (LWEs), the framework offers robust resistance to quantum attacks. The use of CRYSTALS Kyber-768 ensures that even with the advent of quantum computers, the cryptographic security of the EHRs remains intact. This approach enhances privacy and provides a scalable solution for managing health records securely in a post-quantum era.

Mazumdar et al. [53] introduce a quantum-inspired heuristic algorithm combined with Krill Herd Optimisation (QKHO) for healthcare prediction. This model leverages quantum-inspired techniques to enhance the accuracy, precision, recall, and F1-score of healthcare predictions. By integrating blockchain technology, the model ensures secure data transmission to the server, surpassing the security levels of existing RSA and Diffie–Hellman algorithms. The QKHO algorithm provides a highly secure and scalable solution, making it effective against quantum computing threats and improving the overall security of healthcare data transmission.

Chen et al. [54] introduce an Anti-Quantum Attribute-based Signature (AQABS) scheme designed to resist quantum computing attacks in E-health scenarios. The AQABS scheme combines the security of attribute-based signatures with the resilience of quantum-resistant cryptographic techniques. By integrating IPFS with consortium blockchain, the AQABS scheme ensures fully distributed EMR storage, encrypted-EMR searchability, fine-grained access control, low overhead, and utmost scalability. The scheme achieves EMR unforgeability and integrity, signatories' anonymity, and resistance to collusion and quantum computing attacks. Experimental results demonstrate that the AQABS scheme is efficient and lightweight in key extraction, signature generation, and verification overhead compared to existing systems.

Bhavin et al. [55] propose a hybrid scheme that combines blockchain technology with quantum blind signatures to enhance the security of healthcare data. The proposed scheme leverages quantum blind signatures to protect traditional encryption systems from quantum

attacks during block creation using Hyperledger Fabric blockchain. This hybrid approach ensures that healthcare data remain secure against various quantum computing threats. The results show that the proposed scheme improves transaction throughput, reduces resource consumption, and decreases network traffic compared to state-of-the-art schemes.

Wu et al. [56] propose a blockchain-enabled EMR storage management scheme to enhance the security and privacy of healthcare data. The scheme leverages the decentralized and immutable ledger properties of blockchain technology to ensure data integrity, transparency, and robust access control. By integrating smart contracts, the scheme ensures that data access is tightly controlled and transparently logged, mitigating the risks associated with centralized data storage. However, while the scheme effectively addresses classical cybersecurity threats, it remains potentially vulnerable to quantum computing attacks.

These studies highlight various approaches to integrating blockchain and quantum cryptography techniques to secure healthcare data. Table 3 summarizes and compares these studies, emphasising their strengths against quantum attacks, potential risks, and overall impact on healthcare data security.

Table 3. Comparison of blockchain and quantum cryptography techniques for securing healthcare data.

Paper	Approach	Strengths Against Quantum Attack	Risk	Impact
Qu et al. [19]	Quantum cryptography	Uses quantum signatures and quantum identity authentication, leverages quantum cloud computing.	Dependency on quantum cloud computing, potential complexity in implementation.	Enhances security and privacy in IoMT, ensures data integrity, and prevents unauthorized access.
Shuaib et al. [49]	Discusses the broader spectrum of post-quantum cryptography	Highlights the need for quantum-resistant cryptographic algorithms.	Need to transition to quantum-resistant cryptographic algorithms.	Highlights the importance of post-quantum cryptographic solutions.
Liu et al. [50]	Lattice-based cryptography	Employs lattice-based cryptography, introduces a proxy to handle signature generation, incorporates Ethereum blockchain.	Reliance on identity-based cryptography may present a single point of failure.	Reduces computational burden on mobile devices, ensures security and privacy.
Zhao et al. [51]	Code-based cryptography	Utilises Brooks Iyengar quantum Byzantine Agreement-centred blockchain Networking model, employs BBS-OUC cryptosystem and KWBF-QCMDPC algorithm.	Complexity of integrating multiple advanced cryptographic techniques.	Ensures confidentiality and dependability of IoT user data, improves security and scalability.
Bansal et al. [52]	Lattice-based cryptography	Employs CRYSTALS Kyber-768 public key cryptosystem, uses lattice-based cryptography.	Potential computational overhead of CRYSTALS Kyber-768.	Ensures data security, confidentiality, and integrity of EHRs.
Mazumdar et al. [53]	Quantum-inspired heuristic algorithm	Integrates quantum-inspired heuristic algorithm with blockchain technology.	Complexity of quantum-inspired heuristic algorithm.	Guarantees secure data transmission surpasses RSA and Diffie–Hellman algorithms.

Table 3. *Cont.*

Paper	Approach	Strengths Against Quantum Attack	Risk	Impact
Chen et al. [54]	Lattice-based cryptography	Introduces Anti-Quantum Attribute-based Signature (AQABS) scheme, integrates IPFS with consortium blockchain.	Complexity of integrating multiple advanced cryptographic techniques.	Ensures secure and scalable EMR storage and retrieval.
Bhavin et al. [55]	Multivariate polynomial cryptography	Combines blockchain technology with quantum blind signatures, uses Hyperledger Fabric blockchain.	Potential resource consumption and network traffic.	Improves transaction throughput and reduces resource consumption.
Wu et al. [56]	Lattice-based cryptography	Leverages blockchain technology, integrates smart contracts.	Vulnerability to quantum computing attacks.	Improves security, transparency, and access control.
Azzaoui et al. [57]	Hash-based cryptography	Combines Quantum Terminal Machines (QTMs) and blockchain technology, uses Quantum One-Time Pad (Q-OTP) encryption.	Potential vulnerability in converting classical data into quantum bits.	Ensures security and scalability of medical data processing.
Venkatesh et al. [58]	Hash-based cryptography	Utilises quantum cryptographic principles, integrates quantum key distribution and blockchain technology.	Potential high computational cost.	Enhances security, integrity, and privacy of EMRs.
Christo et al. [59]	Quantum cryptography	Combines blockchain technology with quantum cryptography, AES, and SHA algorithms.	Complexity of integrating multiple cryptographic techniques.	Significantly improves security, scalability, and efficiency of healthcare data management.

6.3. Quantum Blockchain-Assisted Privacy Preservation for IoMT

Azzaoui et al. [57] proposed a novel Quantum Cloud-as-a-Service (QCaaS) architecture for secure and efficient processing of medical big data. The architecture combines Quantum Terminal Machines (QTMs) and blockchain technology to ensure security and scalability. QTMs act as intermediaries, converting classical data into quantum bits for processing on quantum servers, while blockchain authenticates and secures communication between nodes. The experimental results confirm that the proposed Quantum One-Time Pad (Q-OTP) encryption-based system can effectively ensure the security of medical data.

Venkatesh and Hanumantha [58] introduced a privacy-preserving quantum blockchain technique for securing electronic medical records (EMRs). The proposed method leverages quantum cryptographic principles to resist various attacks, including intercept, intercept–resend, entangle–measure, man-in-the-middle, collective, and coherent attacks, while reducing communication and computation costs compared to traditional techniques. By integrating quantum key distribution and blockchain technology, the system enhances the security, integrity, and privacy of EMRs, making them resilient to quantum threats.

Qu et al. [19] proposed a QB-IMD system, which integrates quantum blockchain technology to enhance security and privacy in IoMT. This system features a quantum blockchain structure and the QEMR algorithm to ensure data integrity and prevent tampering. The use of quantum signatures and quantum identity authentication provides robust protection against quantum attacks, making it a pioneering solution in post-quantum privacy preservation for medical data. The system also leverages quantum cloud computing for delegated computations, ensuring that diagnostic data are processed without being exposed, thus maintaining user privacy.

Christo et al. [59] propose a hybrid blockchain scheme that combines blockchain technology with quantum cryptography, AES, and SHA algorithms to enhance the security of healthcare data. The proposed scheme employs quantum cryptography for authentication, AES for encryption, and SHA for data retrieval, ensuring robust protection against frequent attacks. The scheme is structured into three phases: authentication, encryption, and data retrieval, leveraging blockchain to provide a secure, decentralized, and transparent system for managing medical records. This approach addresses the vulnerabilities of centralized healthcare systems by ensuring data integrity, confidentiality, and access control. The results indicate that the proposed scheme significantly improves security, scalability, and efficiency in managing healthcare data compared to existing systems.

In Table 3, we compare all the research work discussed in this section on the basis of strengths, risks, and impacts.

7. Discussion and Future Research Directions

The advancements in post-quantum cryptography and blockchain technology have led to innovative solutions for securing healthcare data against quantum threats. The approaches reviewed in this work demonstrate various strategies that combine quantum-resistant cryptographic techniques with blockchain technology that brings decentralisation and immutability. These solutions address the critical need for the enhanced security, privacy, and integrity of electronic medical records and other sensitive healthcare data. The key approaches against quantum attacks discussed in this paper are the following:

1. Post-Quantum Cryptographic Techniques: Several research efforts focused on using post-quantum cryptographic approaches [50,52] employ advanced cryptographic methods, such as lattice-based cryptography, to secure healthcare data. These techniques are resistant to quantum attacks but may introduce additional computational overhead.
2. Integration of Quantum-Inspired Algorithms: Quantum-inspired heuristic algorithms are integrated with blockchain, providing enhanced security measures that surpass traditional algorithms like RSA and Diffie–Hellman [53,58].
3. Quantum Signatures and Quantum Identity Authentication: Solutions such as the QB-IMD system [19] and the advanced IoT security model [51] use quantum signatures and quantum identity authentication to ensure data integrity and prevent tampering in IoMT and IoT environments.
4. Combination of Quantum and Blockchain Technologies: The combination of quantum cryptographic principles with blockchain technology is proposed to enhance security against quantum attacks, which includes using Quantum Terminal Machines and quantum key distribution [57,58].
5. Hybrid and Multi-Phase Approaches: Hybrid schemes combining blockchain with quantum cryptography and other advanced algorithms like AES and SHA are proposed to ensure a multi-layered security approach [55,59].

The above-mentioned approaches provide security and privacy protection to sensitive healthcare data to some degree. Still, there are limitations and challenges that need to be addressed for the security of quantum-secured blockchain systems in healthcare data management. Some of the limitations are as follows:

1. **Research of Post-Quantum Cryptographic Algorithms:** Research-wise, this area has not matured yet as further efforts are required to completely understand the complexity, strengths, and weaknesses of post-quantum cryptographic algorithms like lattice-based cryptography, hash-based cryptography, and other quantum-resistant techniques.
2. **Computational Efficiency:** For both post-quantum and quantum cryptographic algorithms, computational costs can be a limiting factor for their development and adoption. Research focusing on the optimisation of these algorithms is required to ensure they can be implemented efficiently in resource-constrained environments.

3. **Scalability, Interoperability, and Real-World Testing:** Technical and procedural complexities associated with blockchain, cryptographic algorithms, and healthcare data make it difficult to test large-scale solutions. Hence, more efforts are required to test if post-quantum blockchain systems can scale effectively and interoperate with existing healthcare infrastructure. Research should explore ways to integrate these technologies seamlessly into current systems without compromising performance.
4. **Integration of Quantum Key Distribution:** Practical limitations and challenges need to be explored and addressed for integrating QKD into broader healthcare data security frameworks utilising blockchain and other cryptographic protocols.

8. Conclusions

In this work, we delved into the critical domain of privacy preservation for Internet of Medical Things (IoMT)-based healthcare applications. Our study specifically concentrated on blockchain-based solutions, given their potential to provide decentralised, transparent, and immutable frameworks for managing sensitive medical data. We conducted an exhaustive review of the latest research in post-quantum and quantum blockchain-based privacy-preservation techniques tailored to IoMT. By categorizing these research efforts based on the primary security methods employed, we aimed to comprehensively map the current landscape and understand the breadth of strategies being explored. Our findings reveal that numerous innovative approaches show significant promise in safeguarding healthcare data from the threats posed by quantum computing advancements.

Despite these promising developments, our research underscores the imperative need for continued investigation. It is crucial to ensure that these security measures evolve in tandem with new and emerging security threats and are robust enough to defend against unpredictable and unprecedented zero-day attacks. This ongoing research is vital to maintain the integrity and confidentiality of healthcare data in the face of advancing technological threats.

Author Contributions: Conceptualisation, F.S. and S.S.; methodology, F.S. and S.S.; writing—original draft preparation, F.S., S.S., and U.U.T.; writing—review and editing, F.S., S.S., and U.U.T.; supervision, F.S.; project administration, F.S. and S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

EMRs	electronic medical records.
FL	federated learning.
IoMT	Internet of Medical Things.
PQC	post-quantum cryptographic.
PUF	physical unclonable functions.
QCaaS	Quantum Cloud-as-a-Service.
QKD	quantum key distribution.
Q-OTP	Quantum One-Time Pad.
QTMs	Quantum Terminal Machines.

References

1. Cherbal, S.; Zier, A.; Hebal, S.; Louail, L.; Annane, B. Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *J. Supercomput.* **2023**, *80*, 3738–3816. [CrossRef]
2. Khatiwada, P.; Yang, B. An Overview on Security and Privacy of Data in IoMT Devices: Performance Metrics, Merits, Demerits, and Challenges. *pHealth* **2022**, *2022*, 126–136.

3. Selvarajan, S.; Mouratidis, H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci. Rep.* **2023**, *13*, 7107. [CrossRef] [PubMed]
4. Dhinakaran, D.; Srinivasan, L.; Udhaya Sankar, S.; Selvaraj, D. Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis. *Quantum Inf. Comput.* **2024**, *24*, 0227–0266. [CrossRef]
5. Long, B. Classical Solutions for Quantum Challenges: An Introduction to Postquantum Cryptography. *ACM SIGCAS Comput. Soc.* **2024**, *52*, 23–25. [CrossRef]
6. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660. [CrossRef]
7. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [CrossRef]
8. Mukhopadhyay, M.; Banerjee, S.; Mukhopadhyay, C.D. Internet of Medical Things and the Evolution of Healthcare 4.0: Exploring Recent Trends. *J. Electron. Electromed. Eng. Med Inform.* **2024**, *6*, 182–195. [CrossRef]
9. Du, J.; Jiang, C.; Gelenbe, E.; Xu, L.; Li, J.; Ren, Y. Distributed Data Privacy Preservation in IoT Applications. *IEEE Wirel. Commun.* **2018**, *25*, 68–76. [CrossRef]
10. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2021**, *8*, 8707–8718. [CrossRef]
11. 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]
12. Putra, K.T.; Arrayyan, A.Z.; Hayati, N.; Damarjati, C.; Bakar, A.; Chen, H.C. A Review on the Application of Internet of Medical Things in Wearable Personal Health Monitoring: A Cloud-Edge Artificial Intelligence Approach. *IEEE Access* **2024**, *12*, 21437–21452. [CrossRef]
13. Gazi, T. Data to the rescue: How humanitarian aid NGOs should collect information based on the GDPR. *J. Int. Humanit. Action* **2020**, *5*, 9. [CrossRef]
14. Liu, B.; Ding, M.; Shaham, S.; Rahayu, W.; Farokhi, F.; Lin, Z. When machine learning meets privacy: A survey and outlook. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
15. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A trustworthy privacy preserving framework for machine learning in industrial IoT systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6092–6102. [CrossRef]
16. Nair, A.K.; Sahoo, J.; Raj, E.D. Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Comput. Stand. Interfaces* **2023**, *86*, 103720. [CrossRef]
17. Husnoo, M.A.; Anwar, A.; Chakrabortty, R.K.; Doss, R.; Ryan, M.J. Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. *IEEE Access* **2021**, *9*, 153276–153304. [CrossRef]
18. Li, C.; Dong, M.; Xin, X.; Li, J.; Chen, X.B.; Ota, K. Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. *IEEE Internet Things J.* **2023**, *10*, 22051–22064. [CrossRef]
19. Qu, Z.; Meng, Y.; Liu, B.; Muhammad, G.; Tiwari, P. QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT. *IEEE Internet Things J.* **2023**, *11*, 40–49. [CrossRef]
20. Elkhodr, M.; Gide, E.; Darwish, O.; Al-Eidi, S. BioChainReward: A Secure and Incentivised Blockchain Framework for Biomedical Data Sharing. *Int. J. Environ. Res. Public Health* **2023**, *20*, 6825. [CrossRef]
21. Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 710–721. [CrossRef] [PubMed]
22. Ali, A.; Pasha, M.F.; Guerrieri, A.; Guzzo, A.; Sun, X.; Saeed, A.; Hussain, A.; Fortino, G. A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2402–2418. [CrossRef]
23. Saraji, S. Introduction to Blockchain. In *Sustainable Oil and Gas Using Blockchain*; Springer: Cham, Switzerland, 2023; pp. 57–74.
24. Stafford, T.F.; Treiblmaier, H. Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1340–1362. [CrossRef]
25. Storublevtcev, N. Cryptography in blockchain. In Proceedings of the Computational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, 1–4 July 2019; Proceedings, Part II 19; Springer: Cham, Switzerland, 2019; pp. 495–508.
26. Fernández-Caramès, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
27. Aumasson, J.P. The impact of quantum computing on cryptography. *Comput. Fraud Secur.* **2017**, *2017*, 8–11. [CrossRef]
28. Kumar, M. Post-quantum cryptography Algorithm's standardization and performance analysis. *Array* **2022**, *15*, 100242. [CrossRef]
29. Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-quantum lattice-based cryptography implementations: A survey. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 1–41. [CrossRef]
30. Sundaram, B.V.; Ramnath, M.; Prasanth, M.; Sundaram, V. Encryption and hash based security in Internet of Things. In Proceedings of the 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 26–28 March 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.
31. Sendrier, N. Code-based cryptography: State of the art and perspectives. *IEEE Secur. Priv.* **2017**, *15*, 44–50. [CrossRef]

32. Faugère, J.C.; Perret, L. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *J. Symb. Comput.* **2009**, *44*, 1676–1689. [CrossRef]
33. Sood, N. Cryptography in Post Quantum Computing Era. SSRN 4705470. 2024. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4705470 (accessed on 1 May 2024).
34. National Institute of Standardisation and Technology. Available online: https://www.nist.gov/ (accessed on 10 July 2024).
35. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tutor.* **2023**, *26*, 967–1002. [CrossRef]
36. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; IEEE: Piscataway, NJ, USA, 1994; pp. 124–134.
37. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
38. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
39. Rachmawati, D.; Tarigan, J.; Ginting, A. A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. *J. Phys. Conf. Ser.* **2018**, *978*, 012116. [CrossRef]
40. Halak, B.; Gibson, T.; Henley, M.; Botea, C.B.; Heath, B.; Khan, S. Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. *IEEE Access* **2024**, *12*, 8791–8805. [CrossRef]
41. Tasopoulos, G.; Li, J.; Fournaris, A.P.; Zhao, R.K.; Sakzad, A.; Steinfeld, R. Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In Proceedings of the International Conference on Information Security Practice and Experience, Taipei, Taiwan, 23–25 November 2022; Springer: Cham, Switzerland, 2022; pp. 432–451.
42. Satrya, G.B.; Agus, Y.M.; Mnaouer, A.B. A comparative study of post-quantum cryptographic algorithm implementations for secure and efficient energy systems monitoring. *Electronics* **2023**, *12*, 3824. [CrossRef]
43. Mohamed, E.H.; Ankunda, P.V.; Ung, J.; Hwu, W.M. Securing the Internet of Medical Things (IoMT) with K3S and Hybrid Cryptography: Integrating Post-Quantum Approaches for Enhanced Embedded System Security. In Proceedings of the 2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS), Virtual, 19–21 April 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6.
44. Vidaković, M.; Miličević, K. Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments. *Algorithms* **2023**, *16*, 518. [CrossRef]
45. Gharavi, H.; Granjal, J.; Monteiro, E. Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Commun. Surv. Tutorials* **2024**. [CrossRef]
46. Chen, X.; Wang, B.; Li, H. A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security. *J. Inf. Secur. Appl.* **2024**, *81*, 103708. [CrossRef]
47. Li, C.; Jiang, B.; Dong, M.; Xin, X.; Ota, K. Privacy preserving for electronic medical record sharing in healthchain with group signature. *IEEE Syst. J.* **2023**, *17*, 6114–6125. [CrossRef]
48. Yadav, D.K.; Yadav, D.; Pal, Y.; Chaudhary, D.; Sahu, H.; Manasa, A. Post Quantum Blockchain Assisted Privacy Preserving Protocol for Internet of Medical Things. In Proceedings of the 2023 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 29–30 July 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 965–970.
49. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Sam, S.M.; Samy, G.A.N. Effect of quantum computing on blockchain-based electronic health record systems. In Proceedings of the 2022 4th International Conference on Smart Sensors and Application (ICSSA), Penang, Malaysia, 10–12 September 2024; IEEE: Piscataway, NJ, USA, 2022; pp. 179–184.
50. Liu, X.; Luo, Y.; Yang, X.; Wang, L.; Zhang, X. Lattice-Based Proxy-Oriented Public Auditing Scheme for Electronic Health Record in Cloud-Assisted WBANs. *IEEE Syst. J.* **2022**, *16*, 2968–2978. [CrossRef]
51. Zhao, Z.; Li, X.; Luan, B.; Jiang, W.; Gao, W.; Neelakandan, S. Secure internet of things (IoT) using a novel brooks Iyengar quantum byzantine agreement-centered blockchain networking (BIQBA-BCN) model in smart healthcare. *Inf. Sci.* **2023**, *629*, 440–455. [CrossRef]
52. Bansal, A.; Mehra, P.S. A Post-Quantum Consortium Blockchain Based Secure EHR Framework. In Proceedings of the 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 23–24 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.
53. Mazumdar, H.; Chakraborty, C.; Venkatakrishnan, S.B.; Kaushik, A.; Gohel, H.A. Quantum-inspired heuristic algorithm for secure healthcare prediction using blockchain technology. *IEEE J. Biomed. Health Inform.* **2023**, *28*, 3371–3378. [CrossRef] [PubMed]
54. Chen, X.; Xu, S.; Qin, T.; Cui, Y.; Gao, S.; Kong, W. AQ–ABS: Anti-quantum attribute-based signature for EMRs sharing with blockchain. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1176–1181.
55. Bhavin, M.; Tanwar, S.; Sharma, N.; Tyagi, S.; Kumar, N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *J. Inf. Secur. Appl.* **2021**, *56*, 102673. [CrossRef]
56. Wu, G.; Wang, Y. The security and privacy of blockchain-enabled EMR storage management scheme. In Proceedings of the 2020 16th International Conference on Computational Intelligence and Security (CIS), Guangxi, China, 27–30 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 283–287.

57. Azzaoui, A.E.; Sharma, P.K.; Park, J.H. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [CrossRef]
58. Venkatesh, R.; Hanumantha, B.S. A Privacy-Preserving Quantum Blockchain Technique for Electronic Medical Records. *IEEE Eng. Manag. Rev.* **2023**, *51*, 137–144. [CrossRef]
59. Christo, M.S.; Sarathy, P.; Priyanka, C. An efficient data security in medical report using blockchain technology. In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 4–6 April 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 606–610.