XIII SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
ESCA
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 13th INTERNATIONAL CONFERENCE

UMA REVISÃO SISTEMÁTICA DA LITERATURA SOBRE O IMPACTO DA COMPUTAÇÃO QUANTICA NA SEGURANÇA E PRIVACIDADE DE DADOS EM EQUIPAMENTOS DE IOT EM UM CENÁRIO PÓS-QUANTICO

A SYSTEMATIC LITERATURE REVIEW ON THE IMPACT OF QUANTUM COMPUTING ON DATA SECURITY AND PRIVACY IN IOT EQUIPMENT IN A POST-QUANTUM SCENARIO

ANDRE RICARDO CAVALCANTI DE ARAUJO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA - CEFET/RJ

Comunicação:
O XIII SINGEP foi realizado em conjunto com a 13th Conferência Internacional do CIK (CYRUS Institute of Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

UMA REVISÃO SISTEMÁTICA DA LITERATURA SOBRE O IMPACTO DA COMPUTAÇÃO QUANTICA NA SEGURANÇA E PRIVACIDADE DE DADOS EM EQUIPAMENTOS DE IOT EM UM CENÁRIO PÓS-QUANTICO

Objetivo do estudo
Este artigo tem o objetivo de apresentar uma revisão sistemática da literatura sobre a utilização de computação quântica em reder IoT

Relevância/originalidade
A relevância e originalidade consiste na apresentação de uma revisão sistemática que lança foco e considera em igual importância os conceitos de computação quântica, blockchain, segurança e IoT, no recorte temporal estudado.

Metodologia/abordagem
A revisão sistemática da literatura seguiu um protocolo baseado no Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA), realizando a busca em 2 grandes base de dados, selecionando os artigos de conferencia e periódicos com base em seu conteúdo em etapas

Principais resultados
Como resultados, 43 publicações foram selecionadas Descobriu-se que o número de publicações na área cresce rapidamente, Lattice, criptografia pós-quântica (PQC) e distribuição de chaves quânticas (QKD) para proteger redes IoT Internet das Coisas (IoT) são tópicos secundários proeminentes

Contribuições teóricas/metodológicas
Prover compreensão aos acadêmicos e profissionais da área sobre o estado da arte da aplicação da computação quântica, blockchain em redes IoT, tanto em termos da evolução da literatura, como em termos do levantamento de novos desafios de pesquisa

Contribuições sociais/para a gestão
Levantar discussões sobre soluções para problemas de quebra de segurança, envolvendo computação quântica e blockchain reduzindo integridade e privacidade de dados em uso de sensores e internet das coisas.

Palavras-chave: Quantum Computing, Internet of Things, Blockchain, Security, Post-Quantum

A SYSTEMATIC LITERATURE REVIEW ON THE IMPACT OF QUANTUM COMPUTING ON DATA SECURITY AND PRIVACY IN IOT EQUIPMENT IN A POST-QUANTUM SCENARIO

Study purpose
This article aims to present a systematic review of the literature on the use of quantum computing in IoT networks.

Relevance / originality
The relevance and originality consists of the presentation of a systematic review that focuses on and considers the concepts of quantum computing, blockchain, security and IoT with equal importance, within the time frame studied.

Methodology / approach
The systematic literature review followed a protocol based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA), searching two large databases, selecting conference papers and journals based on their content in stages.

Main results
As a result, 43 publications were selected It was found that the number of publications in the area grows rapidly Lattice, post-quantum cryptography (PQC), and quantum key distribution (QKD) for securing IoT networks and IoT are prominent secondary topics.

Theoretical / methodological contributions
Provide understanding to academics and professionals in the field about the state of the art in the application of quantum computing, blockchain in IoT networks, both in terms of the evolution of the literature and in terms of raising new research challenges.

Social / management contributions
Raise discussions on solutions to security breach problems, involving quantum computing and blockchain, reducing data integrity and privacy in the use of sensors and the Internet of Things.

Keywords: Quantum Computing, Internet of Things, Blockchain, Security, Post-Quantum

A SYSTEMATIC LITERATURE REVIEW ON THE IMPACT OF QUANTUM COMPUTING ON DATA SECURITY AND PRIVACY IN IOT EQUIPMENT IN A POST-QUANTUM SCENARIO

1 Introduction

The growing relevance of the Internet of Things (IoT) is increasingly reflected in its integration into daily life. As noted by Souza et al. (2020), IoT encompasses the technological framework that enables everyday objects—such as mobile sensors, smartwatches, home appliances, and even clothing—to connect and communicate through the Internet. Huan and Zukarman (2024) describe IoT as a network of physical devices embedded with sensors and software, facilitating data exchange among interconnected systems. Through the convergence of technologies like sensors and cloud computing, IoT has evolved into a sophisticated information industry ecosystem. Sasaki (2022) estimates that by the end of 2025, approximately 75 billion devices will be connected via IoT. Today, IoT plays a pivotal role in domains such as Industry 4.0, smart societies, artificial intelligence (AI), and the advancement of 6G technologies (Huan and Zukarman, 2024).

Blockchain technology holds significant potential for application across diverse sectors, including legal frameworks, financial services, the food industry, smart assets, banking, and supply chain management (Araujo, 2022; Badr et al., 2018; Kumar & Tripathi, 2019; Wang et al., 2019; Min, 2019). First conceptualized by Nakamoto in 2008 and implemented in 2009, blockchain serves as both a technological foundation and a system architecture. Its rising prominence and widespread adoption in recent years are largely attributed to three core attributes: (i) the guarantee of data immutability and integrity, (ii) the removal of reliance on centralized third-party authorities, and (iii) the facilitation of decentralized and reliable transactions (Araujo, 2022; Abujamra & Randall, 2019; Banerjee et al., 2018; Zhang et al., 2018). Blockchain functions by maintaining distributed ledgers shared among participants in a decentralized network, creating a secure and tamper-resistant audit trail. It records IoT sensor outputs—such as payment records, personal data, and contractual agreements—as blockchain transactions (Ali et al., 2019). Using cryptographic algorithms, blockchain ensures robust security, data integrity, and traceability within digital systems.

Quantum computing is emerging as a transformative technology with the potential to disrupt industries and reshape markets on a global scale. A recent McKinsey report (2025) projects that the quantum computing market could reach a valuation of USD 2 trillion by 2035, with the most profound effects anticipated in finance, chemistry, pharmaceuticals, and the automotive industry. Leading tech companies are already investing billions in quantum research and development, and many are providing partial public access to quantum systems via cloud-based platforms (Rahmani, 2018). Unlike classical computers, quantum systems harness core principles of quantum mechanics—such as superposition and entanglement—to encode and process data (Rahmani, 2018). These phenomena enable quantum computers to solve highly complex and specialized problems at speeds unattainable by traditional computing. Additionally, interference plays a vital role in retrieving information from quantum states (Aaronson, 2008). Given these capabilities, quantum computing is poised to revolutionize the field of information technology and may become a cornerstone of the anticipated "Fifth Industrial Revolution" (Rahmani, 2018).

In this sense, given the novelty of this field of research, the research questions approached by this article emerge. These research questions are: How does the literature regarding the application of Quantum Computing blockchain in IoT scenario have been performing in recent years? And what are the potential challenges and future research directions regarding the application of Quantum computing blockchain in IoT security?

Given the research questions, the general objective of this article is to perform a systematic literature review to unravel the state-of-the-art research on the application of Quantum computing blockchain in IoT communication. The specific objectives of this article are the ones that follow. First, to show the bibliometric evolution of publications regarding the usage of quantum computing in IoT devices. Second, to indicate the potential challenges and future research directions regarding the application of quantum computing blockchain in IoT.

The remainder of this article is organized as follows. In Section 2, the background on quantum computing and IoT is presented. In Section 3, the research methodology is presented. In Section 4, research results are presented and discussed. Section 5 concludes this work and draws future directions.

2 Theoretical backgrounds

This section introduces the basic concepts and background on the main subjects approached by our work. Section 2.1 discusses quantum computing technology, and Section 2.2 discusses cryptography technology.

2.1 Quantum Computing.

Quantum computing represents a new paradigm in information processing, grounded in the principles of quantum physics. Unlike classical computing, which encodes data using bits that exist as either 0 or 1 (Bernhardt, 2019), quantum computers utilize quantum bits—or qubits—that can exist in a state of both 0 and 1 simultaneously, a phenomenon known as superposition. Another foundational concept, entanglement, allows qubits to become interconnected in such a way that the state of one instantly influences the state of another, even across vast distances (Gill et al., 2022).

According to these unique properties, quantum computers can perform certain types of calculations significantly faster than their classical counterparts. They are particularly well-suited for tasks such as simulating quantum systems, solving complex cryptographic challenges, and addressing optimization problems (Cusumano, 2018).

In the context of the Internet of Things (IoT), quantum computing introduces transformative possibilities for enhancing security. It offers a new approach to cryptography that strengthens the protection of IoT devices and networks. Traditional encryption methods rely on the computational difficulty of specific mathematical problems. However, quantum computers can solve these problems exponentially faster, rendering many classical cryptographic techniques vulnerable (Bhatt and Sharma, 2019).

2.2 Cryptography

Cryptography is the science of securing communication and data using mathematical algorithms and protocols. Its origins trace back thousands of years, serving as a vital tool for protecting sensitive information. At its core, cryptography involves encoding messages or data using complex mathematical techniques, rendering them unreadable to unauthorized parties without the correct key or password. The two primary categories of cryptography are symmetric key cryptography and public key cryptography (Mousavi et al., 2021).

Symmetric key cryptography—also known as secret key cryptography—relies on a single shared key for both encryption and decryption. One of the most widely adopted algorithms in this category is the Advanced Encryption Standard (AES), known for its speed and security.

In contrast, public key cryptography (or asymmetric cryptography) uses a pair of keys: a public key for encryption and a private key for decryption. The RSA algorithm, which leverages the mathematical properties of prime numbers, is the most used public key encryption method. This approach is essential for secure online transactions and digital signatures.

Another important cryptographic technique is the use of hash functions, which play a crucial role in technologies like blockchain. A hash function transforms an input message or dataset into a fixed-length string, or hash, that is uniquely tied to the original input. Even a minor alteration in the input produces a drastically different hash, making unauthorized changes easily detectable (Almazrooie et al., 2020). The Secure Hash Algorithm (SHA) is a widely used hash function, instrumental in verifying the authenticity of digital signatures and other forms of data.

3 Research methodology

To provide a transparent, reproducible, and scientific literature review, the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) protocol was followed in this work (Moher et al., 2009). The first step in the systematic mapping process was defining the research questions based on the objectives of this work.

Research Question 1 - How the literature regarding the application of quantum computing in the IoT devices has been performing in recent years?

Research Question 2 - What are the potential challenges and future research directions regarding the application of quantum computing in the IoT data privacy devices?

The second step was defining the scientific databases where to perform the search for articles. The database chosen for searching the research strings were Scopus, which is the largest database of peer-reviewed literature and recovers journals from all major databases such as Emerald, Taylor & Francis, Science Direct, PubMed, among others (Chadegani, et al., 2013) and ISI Web of Science which is not as large as Scopus but can recover papers from a greater year range and has citation database and publication that covers all domains of science for many years (Chadegani, et al., 2013). Study of Vieira and Gomes (2009) reveals that 2/3 of the studies can be found in both databases and 1/3 only in one database. Another considerable advantage is that both databases provide “. bib” files providing full search data (such as references, article authors, etc.) that can be further analyzed in bibliometric packages.

The third step was to define search terms and search string used to perform the search on the selected databases. The final search string used was “((Blockchain OR “Smart Contract” OR Ledger) AND ("Cloud" OR "Fog" OR "Edge" OR "Sensor" OR "Internet of ") AND Quantum) AND ("Secur" OR "Crypto" OR "Sign"). This search string was constructed based on the research domains of this work (Quantum Computing, Blockchain, Security and IoT). Nevertheless, even conducting the research in both databases it would not be possible to guarantee that all relevant literature was covered and so, it can be considered a limitation. The second limitation is that only papers in English language were considered. This decision was taken based in: i) Most review articles (and all review articles in this thesis) use this criterion, therefore, it has literature methodological support, ii) English is the main language used to communicate scientific research, iii) To guarantee that any researcher can understand any paper selected for this bibliometric study. As the main limitations, can be cited the fact that were reviewed international journal articles (published in the English language), excluding conference papers, master and doctoral dissertations, textbooks, book chapters, unpublished articles and notes, and excluded publication from 2025 year, due to incomplete year end it was added the AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "re")) AND (LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (PUBYEAR , 2025)) string.

Table 1

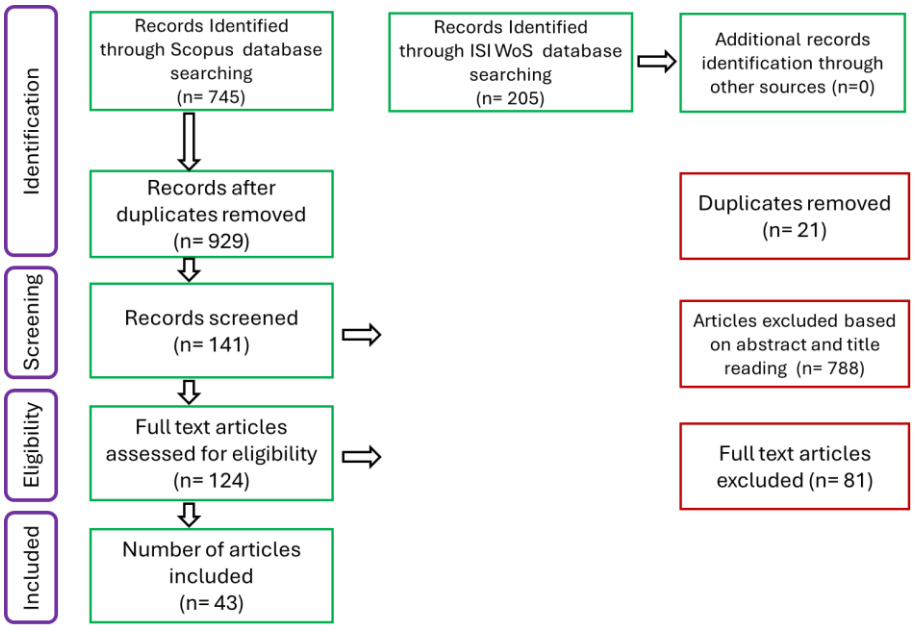
First Seach result

Scientific data source	Raw Results
Scopus	745
Web of Science	205
Total	950

Note: Source: the author

The fourth step was to perform the search in the databases, obtaining BibTeX files. The fifth step was to import all the retrieved BibTeX files that were generated by the databases after each search with the search results into the reference management software Mendeley® (https://www.mendeley.com, accessed in 29, June 2025). The number of paper results following the PRISMA protocol are shown in figure 1.

Figure 1
Research flow datagram



Note: Source: the author

The sixth step was to conduct the "first selection" process on all the papers of both databases. In this first selection, 21 papers were excluded due duplication, and 788 papers were excluded after record screening (Title and Abstract Review) detail by reading their titles and abstracts, assessing if the papers met the relevance criterion, i.e. papers which did not focus on the application of quantum computing, blockchain communication of IoT, according to their title and abstracts were removed. The remaining papers were 141, but due access restrictions only 124 papers were downloaded and fully read, using the same relevance criterion. The final list has 43 screened papers, which will be assessed in the following section of this work.

4 Results of the systematic literature review

This section shows the results of this research regarding the 43 final papers screened. Sections 4.1 and 4.2 discuss the results regarding, respectively, research questions 1 and 2, and provide answers to such questions.

4.1 Performance of literature on quantum computing in IoT devices.

Even though the search period started in 2018, there are no publications regarding Quantum computing, blockchain and the IoT topics together in that year. Figure 2 shows the

distribution of papers throughout the years. The papers started to be published in 2019 and few others published in 2020 and 2021, with a reduced number of publications in 2021, coincidentally during the pandemic period. due to COVID-19 pandemic. The majority of published papers is from 2021 (21 papers, i.e. 48,83% of publications. This result shows that the research on quantum computing in IoT is a new topic and the number of published papers in this topic is growing fast.

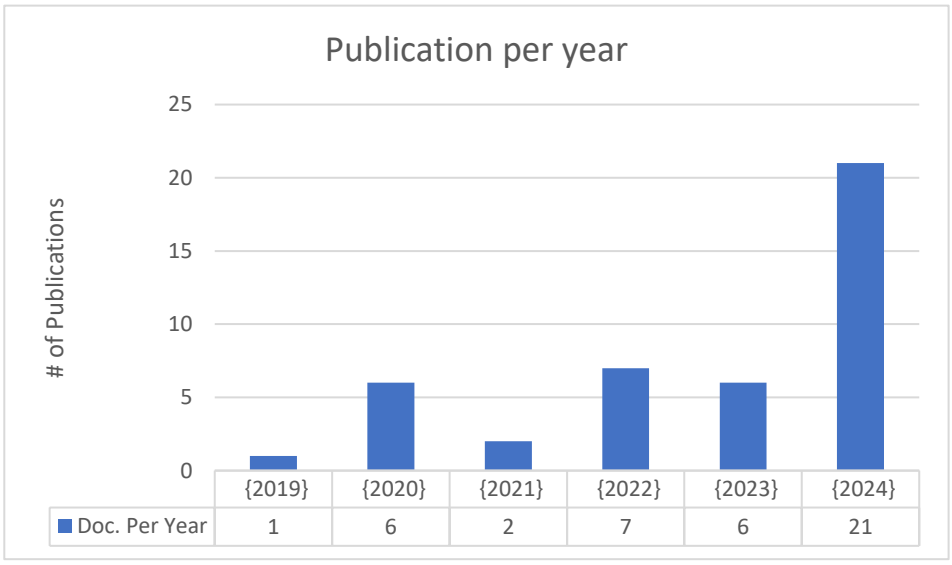


Figure 2: Number of papers published (# of Publication) by year of publication
Source: the authors

This research considers some different scientific areas (Engineering, Computer Science, Physics, Business,), represented by the scientific data sources selected. Most of the selected papers (29, i.e. 67,40% of the 43 papers screened) were published in Engineering and Computer Science. This suggests that academics from those areas are interested in the application of quantum computing blockchain in IoT.

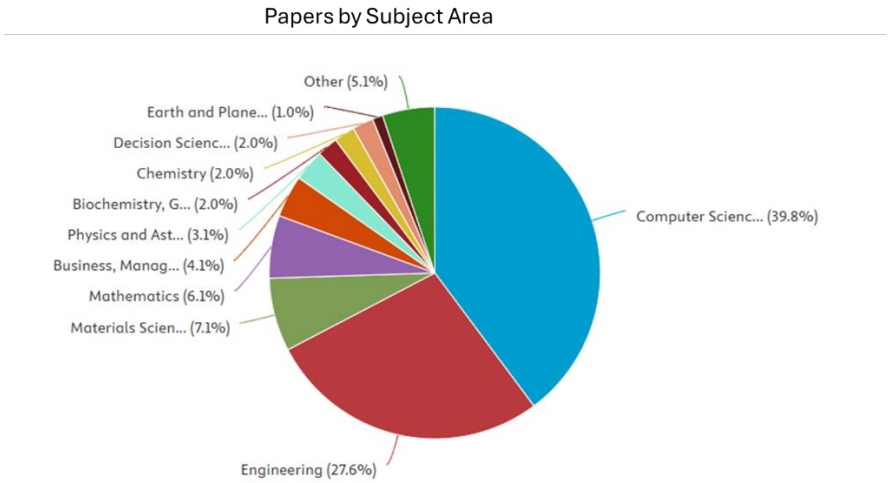


Figure 3: Number of papers published per area
Source: the author using scopus analyses

4.2 Challenges and future research directions on quantum computing blockchain in IoT

Publication in this area started in 2019 (Li, et al., 2019) regarding vulnerability of cryptography algorithm applied in blockchain or Blockchain Internet of Things (BIoT) using quantum computing technology. Several researchers (44,18 % of papers) have highlighted the potential of using quantum computing or lattice cryptography (Tao, et al., 2023; Yu, et al., 2022; Li, et al., 2019; Gupta, et al., 2022, and other).

According to the research, quantum computing can be applied within healthcare management applications with blockchain IoT Medical devices (IoMT) in public or private areas, monitoring and automating health claims adjudication and online patient information, achievement of healthcare records, sharing patients' medical data information, pharmaceutical and drug medicine counterfeiting, medical clinical trial, and precision medicine. (Qu, et al., 2022; Qu, et al., 2024; Casino et al., 2019; Badr et al., 2018; Sabrina, et al., 2024). Combining blockchain technology and the healthcare supply chain allows solving problems of scientific credibility of losing information (data missing or dredging, endpoint switching and selective publication) in clinical trials (Benchoufi & Ravaud, 2017) as well as issues of patients' informed consent.

Based on the 43 papers screened, IoT technologies and sensors seem to be a representative new worry about security into post quantum scenarios. The blockchain technology used to be a strong method of integrity, security and trackability, but the new compute paradigm quantum computers use quantum phenomena (entanglement and superposition) to achieve computation which can be applied to classical computational problems, such as to the cipher algorithms, or entirely novel paradigms can be designed such as in the emerging quantum cryptography.

Therefore, the first challenge that emerges on the application of quantum computing blockchain in IoT is how to use blockchain technology to keep secure in a post quantum scenario. The development of Post Quantic Cryptography (PQC) and/or Quantum Key Distribution (QKD) to protect IoT Network devices (Yang, et al., 2024; Dhar, et al., 2024) can be a novel approach.

A second challenge that emerges on the application of quantum computing blockchain is refers to how to build a framework based on Quantum blockchain to meet accuracy and integrity requirements of security. It is also possible to develop a Quantum Blockchain Internet of Things (QBIoT) (Li, et al., 2024) to reference and use in all kind of IoT Network, for example, drones IoT, Vehicular IoT, Medical IoT, Industrial IoT and others

A third challenge that emerges on the application of lattice cryptography to attend the security issues in a post quantum scenario may comprise, besides ensuring the accuracy of data collected and maintaining the integrity of exchanged information, the processing of large amounts of data, along with the reduction in the response time of applications. However, further implementations and evaluations in real scenarios are still necessary.

5 Conclusion

This paper presented a systematic literature review on the application of quantum computing blockchain in Internet of things devices. The systematic literature review followed a protocol based on PRISMA. The first research question referred to investigating the bibliometric evolution of publications regarding the usage of quantum computing blockchain in IoT. The second research question referred to indicating the potential challenges and future research directions regarding the application of quantum computing technology to protect IoT

devices communication. As results, there are few publications (43) with quantum computing, blockchain and IoT directly involved between 2019 and 2024, limited by 2024 year. The topic is relatively new. The results show that research in this field is growing rapidly as the number of publications has increased in most recent years, and there is much interest from specialists from the areas of engineering and computer science. In addition, the potential benefits of quantum computing to protect blockchain performance to several applications in the IoT were raised. Three challenges were raised regarding (i) the usage of lattice technology to protect consensus mechanisms, (ii) a framework to provide security in post quantum scenario, and (iii) the development of novel quantum computed technologies scenarios. As a future research direction of this work, it is suggested the research of solutions for each of these challenges. Another research direction refers to performing another systematic review including the 2025 completed year papers.

6 References

Abd El-Latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., & Peng, J. (2021). **Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities**. Information Processing and Management, 58(4). https://doi.org/10.1016/j.ipm.2021.102549

Abujamra, R. & Randall, D., (2019). **Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework**. In: Advances in Computers. s.l.:Elsevier.

Agbo, C., Mahmoud, Q. & Eklund, J., (2019). **Blockchain Technology in Healthcare: A Systematic Review**. Healthcare, 4 4, 7(2), p. 56.

Almazrooie M, Samsudin A, Gutub AA-A, Salleh MS, Omar MA, Hassan SA (2020) **Integrity verification for digital holy quran verses using cryptographic hash function and compression**. J King Saud Univ-Comput and Inf Sci 32(1):24–34

Althobaiti, O. S., & Dohler, M. (2020). **Cybersecurity challenges associated with the internet of things in a post-quantum world**. IEEE Access, 8, 157356–157381. https://doi.org/10.1109/ACCESS.2020.3019345

Anbarkhan, S. H. (2024). **Securing IoT Networks: A Post-Quantum Blockchain and Deep Learning Approach for Enhanced Cyber Defense**. International Journal of Safety and Security Engineering, 14(6), 1689–1698. https://doi.org/10.18280/ijsse.140604

Araujo, A. R. C, 2022, **A Systematic Review on the Blockchain-Enabled Cloud of Sensors in Healthcare**, Master's thesis at CEFET-RJ

Azzi, R., Kilany,, R. Sokhn, M.,(2019) **The power of a blockchain-based supply chain**. Computers & Industrial Engineering.

Badr, S., Gomaa, I. & Abd-Elrahman, E., (2018). **Multi-tier blockchain framework for IoT-EHRs systems**. s.l., Elsevier B.V., pp. 159-166.

Bagchi, P., Maheshwari, R., Bera, B., Das, A. K., Park, Y., Lorenz, P., & Yau, D. K. Y. (2023). **Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications**. IEEE Transactions on Vehicular Technology, 72(8), 10393–10408. https://doi.org/10.1109/TVT.2023.3260579

Balogh, S., Gallo, O., Ploszek, R., Špaček, P., & Zajac, P. (2021). **Iot security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques**. In Electronics (Switzerland) (Vol. 10, Issue 21). MDPI. https://doi.org/10.3390/electronics10212647

Banerjee, M., Lee, J. & Choo, K. K. R., (2018). **A blockchain future for internet of things security: a position paper**. Digital Communications and Networks, 1 8, 4(3), pp. 149-160.

Benchoufi, M. & Ravaud, P., (2017). **Blockchain technology for improving clinical research quality.** Trials, 18(1).

Bernhardt C (2019) **Quantum computing for everyone**. Mit Press

Bhatt AP, Sharma A (2019) **Quantum cryptography for internet of things security**. J Electr Sci and Technol 17(3):213–220

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab , M.,(2020). **Blockchain for Industry 4.0: A comprehensive review**. IEEE Access, v. 8, p. 79764–79800, 2020. Accessed in: https://doi.org/10.1109/ACCESS.2020.2988579

Broadbent A, Schaffner C (2016) **Quantum cryptography beyond quantum key distribution**. Des Codes Crypt 78:351–382

Brogan, J., Baskaran, I. & Ramachandran, N., (2018). **Authenticating Health Activity Data Using Distributed Ledger Technologies.** Computational and Structural Biotechnology Journal, 1 1, Volume 16, pp. 257-266.

Casino, F., Dasaklis, T. K. & Patsakis, C., (2019). **A systematic literature review of blockchain-based applications: Current status, classification and open issues**. s.l.:Elsevier Ltd.

CHADEGANI, A.; SALEHI, H.; YUNUS, M. M.; FARHADI, H.; FOOLADI, M.; FARHADI, M.; ALE EBRAHIM, N. A **comparison between two main academic literature collections: Web of science and scopus databases**. Asian Social Science, v. 9, n. 5, p. 18-26, 2013.

Chawla, D., & Mehra, P. S. (2023). **A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions**. In Internet of Things (Netherlands) (Vol. 24). Elsevier B.V. https://doi.org/10.1016/j.iot.2023.100950

Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S., (2018). **Blockchain-Based Medical Records Secure Storage and Medical Service Framework**. Journal of Medical Systems, 11.43(1).

Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). **Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing**. Journal of Supercomputing, 80(3), 3738–3816. https://doi.org/10.1007/s11227-023-05616-2

Christidis, K. and Devetsikiotis, M. (2016), **Blockchains and smart contracts for the internet of things**, IEEE Access, Special Section on the Plethora of Research in IoT, Vol. 4, pp. 2292-2303.

Cusumano MA (2018) **The business of quantum computing**. Commun ACM 61(10):20–22

Dhanvijay, MM., Patil, SC,. (2019): **Internet of Things: A survey of enabling technologies in healthcare and its applications,** Computer Networks, Volume 153.

Dhar, S., Khare, A., Dwivedi, A. D., & Singh, R. (2024). **Securing IoT devices: A novel approach using blockchain and quantum cryptography**. Internet of Things (Netherlands), 25. https://doi.org/10.1016/j.iot.2023.101019

Dhinakaran, D., Srinivasan, L., Udhaya Sankar, S. M., & Selvaraj, D. (2024). **QUANTUM-BASED PRIVACY-PRESERVING TECHNIQUES FOR SECURE AND TRUSTWORTHY INTERNET OF MEDICAL THINGS: AN EXTENSIVE ANALYSIS**. In Quantum Information and Computation (Vol. 24, Issue 4).

Dwivedi, A. D., Srivastava, G., Dhar, S. & Singh, R., (2019). **A decentralized privacy-preserving healthcare blockchain for IoT**. Sensors (Switzerland), 1.19(2).

Fernandez-Carames, T. M. (2020). **From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things**. In IEEE Internet of Things Journal (Vol. 7, Issue 7, pp. 6457–6480). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2019.2958788

Galvez, J. F., Mejuto, J. C. & Simal-Gandara, J., (2018). **Future challenges on the use of blockchain for food traceability analysis**. s.l.:Elsevier B.V..

Gharavi, H., Granjal, J., & Monteiro, E. (2024). **Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions**. IEEE Communications Surveys and Tutorials, 26(3), 1748–1774. https://doi.org/10.1109/COMST.2024.3355222

Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, Buyya R (2022) **Quantum computing: a taxonomy, systematic review and future directions**. Software: Practice and Exper 52(1):66–114

Gomes, A., Senna, P., Monteiro, A., Pinha, D., (2016). **Study on techniques and tools used in lean healthcare implementation: A literature review**. Brazilian Journal of Operations & Production Management, v. 13, n. 4, p. 406, 2016. Accessed in https://doi.org/10.14488/BJOPM.2016.v13.n4.a1

Gordon, W. J. & Catalini, C., (2018). **Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability**. Computational and structural biotechnology journal.

Gupta, D. S., Karati, A., Saad, W., & da Costa, D. B. (2022). **Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles**. IEEE Transactions on Vehicular Technology, 71(3), 3255–3266. https://doi.org/10.1109/TVT.2022.3144785

Gupta, D. S., Ray, S., Singh, T., & Kumari, M. (2022). **Post-quantum lightweight identity-based two-party authenticated key exchange protocol for Internet of Vehicles with probable security**. Computer Communications, 181, 69–79. https://doi.org/10.1016/j.comcom.2021.09.031

Hölbl, M., Kompara, M., Kamišalić, A. & Zlatolas, L. N., (2018). **A systematic review of the use of blockchain in healthcare**. Symmetry, 10(10).

Hussein, A. I., MaoLood, A. T., & Gbash, E. K. (2024). **A Systematic Review: Post Quantum Cryptography to Secure Data Transmission**. In Iraqi Journal of Science (Vol. 65, Issue 7, pp. 3975–3992). University of Baghdad-College of Science. https://doi.org/10.24996/ijs.2024.65.7.35

Jagdale, B., Sugave, S. R., Kulkarni, Y. R., & Gutte, V. (2024). **Privacy-aware quantum convolutional neural network for blockchain-based IoT health care data**. Intelligent Decision Technologies, 18(2), 1337–1354. https://doi.org/10.3233/IDT-230386

Kamel Boulos, M. N., Wilson, J. T. & Clauson, K. A., (2018). **Geospatial blockchain: promises, challenges, and scenarios in health and healthcare**. International journal of health geographics, 17(1), p. 25.

Keers RN, Williams SD, Cooke J, Ashcroft DM.(2013). **Prevalence and nature of medication administration errors in health care settings: a systematic review of direct observational evidence**. Ann Pharmacother. 2013 ;47:237–256

Krähenbühl-Melcher A, Schlienger R, Lampert M, Hascke, M., Drewe J., Krahenbuhl S.,(2007) **Drug-related problems in hospitals: a review of the recent literature**. Drug Saf. 2007 ;30:379–407.

Kshetri, N. (2018) **Blockchain's roles in meeting key supply chain management objectives**, International Journal of Information Management, Vol. 39 (April), pp. 80-89.

Kumar, R. & Tripathi, R., (2019). **Traceability of counterfeit medicine supply chain through Blockchain.** s.l., s.n., pp. 568-570.

Kuo, T. T., Kim, H. E. & Ohno-Machado, L.,(2017). **Blockchain distributed ledger technologies for biomedical and health care applications**. Journal of the American Medical Informatics Association, 11, 24(6), pp. 1211-1220.

Lambert, D. M., Cooper, M. C., (2000). **Issues in Supply Chain Management**, Industrial Marketing Management 29, 65–83

Li, C., Xu, G., Chen, Y., Ahmad, H., & Li, J. (2019). **A new anti-quantum proxy blind signature for blockchain-enabled internet of things**. Computers, Materials and Continua, 61(2), 711–726. https://doi.org/10.32604/cmc.2019.06279

Li, J., Nong, Q., & Liu, Z. (2024). **QBDD: Quantum-resistant blockchain-assisted deep data deduplication protocol for vehicular crowdsensing system**. Computer Networks, 245. https://doi.org/10.1016/j.comnet.2024.110393

Liu, A., Chen, X. B., Xu, G., Wang, Z., Sun, Y., Wang, Y., & Feng, H. (2024). **QBIoV: a secure data sharing scheme for the Internet of vehicles based on quantum-enabled blockchain**. Quantum Information Processing, 23(6). https://doi.org/10.1007/s11128-024-04432-8

Liu, A., Zhang, Q., Xu, S., Feng, H., Chen, X. B., & Liu, W. (2024). QBIoT: **A Quantum Blockchain Framework for IoT with an Improved Proof-of-Authority Consensus Algorithm and a Public-Key Quantum Signature**. Computers, Materials and Continua, 80(1), 1727–1751. https://doi.org/10.32604/cmc.2024.051233

Liu, J., Wen, J., Zhang, B., Dong, S., Tang, B., & Yu, Y. (2023). **A post quantum secure multi-party collaborative signature with deterability in the Industrial Internet of Things**. Future Generation Computer Systems, 141, 663–676. https://doi.org/10.1016/j.future.2022.11.034

Lohachab, A., Lohachab, A., & Jangra, A. (2020). **A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks**. In Internet of Things (Netherlands) (Vol. 9). Elsevier B.V. https://doi.org/10.1016/j.iot.2020.100174

Min, H., (2019). **Blockchain technology for enhancing supply chain resilience**. Business Horizons, 1 1, 62(1), pp. 35-45.

Mohanty, T., Srivastava, V., Debnath, S. K., Das, A. K., & Sikdar, B. (2024). **Quantum Secure Threshold Private Set Intersection Protocol for IoT-Enabled Privacy-Preserving Ride-Sharing Application**. IEEE Internet of Things Journal, 11(1), 1761–1772. https://doi.org/10.1109/JIOT.2023.3291132

Mohed, D., Liberati, A., Tetzlaff, J., Altman, D. G.,(2009) **Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement**. PLoS Medicine, v. 6, n. 7, p. 1-9, 2009.

Mousavi SK, Ghaffari A, Besharat S, Afshari H (2021) **Security of internet of things based on cryptographic algorithms: a survey**. Wireless Netw 27:1515–1555

Mustafa, I., Khan, I. U., Aslam, S., Sajid, A., Mohsin, S. M., Awais, M., & Qureshi, M. B. (2020). **A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications**. IEEE Access, 8, 99273–99285. https://doi.org/10.1109/ACCESS.2020.2995801

N. Reibling, M. Ariaans, C. Wendt, (2019). **Worlds of Healthcare: A Healthcare System Typology of OECD Countries**, Health Policy, Volume 123, Issue 7, Pages 611-620,

Nakamoto S.; (2008) **Bitcoin: A peer-to-peer electronic cash system**. https://bitcoin.org/bitcoin.pdf, Accessed: 2018-Dec-01.

Nofer, M., Gomber, P., Hinz, O., Schiereck, D., (2017) **Blockchain. Business & Information Systems Engineering**, v. 59, n. 3, p. 183–187, 2017. Accessed in : https://doi.org/10.1007/s12599-017-0467-3

P.E. Plsek, T. Greenhalgh, (2001). **The challenge of complexity in health care. BMJ**: British Medical Journal, 323 (7313), pp. 625-628

Peelam, M. S., & Chamola, V. (2024). **Enhancing Security Using Quantum Blockchain in Consumer IoT Networks**. IEEE Transactions on Consumer Electronics. https://doi.org/10.1109/TCE.2024.3512791

Prajapat, S., Kumar, P., Kumar, D., Das, A. K., Shamim Hossain, M., & Rodrigues, J. J. P. C. (2024). **Quantum Secure Authentication Scheme for Internet of Medical Things Using Blockchain**. IEEE Internet of Things Journal, 11(23), 38496–38507. https://doi.org/10.1109/JIOT.2024.3448212

Qu, Z., Shi, W., Liu, B., Gupta, D., & Tiwari, P. (2024). **IoMT-Based Smart Healthcare Detection System Driven by Quantum Blockchain and Quantum Neural Network**. IEEE Journal of Biomedical and Health Informatics, 28(6), 3317–3328. https://doi.org/10.1109/JBHI.2023.3288199

Qu, Z., Zhang, Z., & Zheng, M. (2022). **A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things**. Information Sciences, 612, 942–958. https://doi.org/10.1016/j.ins.2022.09.028

Radanovic & Likic, (2018). **Opportunities for Use of Blockchain Technology in Medicine**. Applied Health Economics and Health Policy, 16(5), pp. 583-590.

Sabrina, F., Sohail, S., & Tariq, U. U. (2024). **A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain.** In Electronics (Switzerland) (Vol. 13, Issue 15). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13152962

Santos, I. L., Pirmez, L., Delicato, F. C., Oliveira, G. M., Farias, C. M., Khan, S. U., Zomaya, A. Y.,(2018). **Zeus: A resource allocation algorithm for the cloud of sensors**. Future Generation Computer Systems, 2018. Accessed in: https://doi.org/10.1016/j.future.2018.03.026

Schepel, L., Aronpuro, K., Kvarnström, K., Holmström A.R., Airaksinen M. (2019) **Strategies for improving medication safety in hospitals: Evolution of clinical pharmacy services**. Research in Social and Administrative Pharmacy, In press, corrected proof

Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). **Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey**. Cluster Computing, 25(3), 1729–1748. https://doi.org/10.1007/s10586-021-03380-7

Shahid, F., Khan, A., & Jeon, G. (2020). **Post-quantum distributed ledger for internet of things.** Computers and Electrical Engineering, 83. https://doi.org/10.1016/j.compeleceng.2020.106581

Shahidinejad, A., & Abawajy, J. (2023). **Decentralized Lattice-Based Device-to-Device Authentication for the Edge-Enabled IoT**. IEEE Systems Journal, 17(4), 6623–6633. https://doi.org/10.1109/JSYST.2023.3319280

Singh, S. K., Azzaoui, A. el, Salim, M. M., & Park, J. H. (2020). **Quantum Communication Technology for Future ICT - Review.** Journal of Information Processing Systems, 16(6), 1459–1478. https://doi.org/10.3745/JIPS.03.0154

Tandel, P., & Nasriwala, J. (2024). **Secure authentication framework for IoT applications using a hash-based post-quantum signature scheme**. Service Oriented Computing and Applications. https://doi.org/10.1007/s11761-024-00414-x

Tanwar, S., Parekh, K., Evans, R.,(2020) **Blockchain-based electronic healthcare record system for healthcare 4.0 applications**. Journal of Information Security and Applications, v. 50, 2020. Accessed in: https://doi.org/10.1016/j.jisa.2019.102407

Tao, X., Qiang, Y., Wang, P., & Wang, Y. (2023). **LMIBE: Lattice-Based Matchmaking Identity-Based Encryption for Internet of Things**. IEEE Access, 11, 9851–9858. https://doi.org/10.1109/ACCESS.2023.3240304

Tapscott D, Tapscott A. (2016.) **Blockchain Revolution: How the Technology behind Bitcoin** Is Changing Money, Business, and the World. New York: Penguin;

Tseng, J. H., Liao, Y. C., Chong, B. & Liao, S. W., (2018). **Governance on the drug supply chain via gcoin blockchain**. International Journal of Environmental Research and Public Health, 6.15(6).

Vazirani, A. A., O'Donoghue, O., Brindley, D. & Meinert, E., (2019). **Implementing Blockchains for Efficient Health Care: Systematic Review**. Journal of medical Internet research, 2, 21(2), p. e12439.

VIEIRA, E. S.; GOMES, J. A. N. F. **A comparison of Scopus and Web of Science for a typical university**. Scientometrics, v. 81, n. 2, p. 587-600, 2009.

Vimala Josphine, C., Theodore Kingslin, M., Fatima Vincy, R., Mohana, M., & Babitha, S. (2024). **Efficient quantum inspired blockchain-based cyber security framework in IoT using deep learning and huristic algorithms**. Intelligent Decision Technologies, 18(2), 1203–1232. https://doi.org/10.3233/IDT-230579

Wang, Y., Singgih, M., Wang, J. & Rit, M., (2019). **Making sense of blockchain technology: How will it transform supply chains?**. International Journal of Production Economics, 1 5, Volume 211, pp. 221-236.

Wazid, M., Das, A. K., & Park, Y. (2024). **Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future**

Research. IEEE Open Journal of the Computer Society, 5, 248–267. https://doi.org/10.1109/OJCS.2024.3397307

Westbrook J, Rob M, Woods A, Parry D., (2011) **Errors in the administration of intravenous medications in hospital and the role of correct procedures and nurse experience**. BMJ Qual Saf. 2011 ;20:1027–1034.

Xu, S., Wang, T., Sun, A., Tong, Y., Ren, Z., Zhu, R., & Song, H. H. (2024). **Post-Quantum Anonymous, Traceable and Linkable Authentication Scheme Based on Blockchain for Intelligent Vehicular Transportation Systems**. IEEE Transactions on Intelligent Transportation Systems, 25(9), 12108–12119. https://doi.org/10.1109/TITS.2024.3383668

Yadav, D. K., Sahu, H., Chaudhary, D., & Lee, C. C. (2024). **Module lattice based post quantum secure blockchain empowered vehicle to vehicle communication in the internet of vehicles**. Computers and Electrical Engineering, 117. https://doi.org/10.1016/j.compeleceng.2024.109245

Yang, Z., Shi, Q., Cheng, T., Zhang, Q., Liu, Q., Liu, Y., & Peng, S. (2024). QBMA-BIV: **Quantum-Key-Distribution (QKD)-Based Multi-Server Authentication Scheme for Blockchain-Enabled Internet of Vehicles**. IEEE Transactions on Intelligent Transportation Systems, 25(11), 18433–18448. https://doi.org/10.1109/TITS.2024.3432772

Ye, F., Zhou, Z., & Li, Y. (2022). **Quantum-assisted blockchain for IoT based on quantum signature**. Quantum Information Processing, 21(9). https://doi.org/10.1007/s11128-022-03676-6

Yi, H. (2022). **Secure Social Internet of Things Based on Post-Quantum Blockchain**. IEEE Transactions on Network Science and Engineering, 9(3), 950–957. https://doi.org/10.1109/TNSE.2021.3095192

Yu, W., Yang, L., & Wang, S. (2022). **New Lattice-Based Broadcast Authentication Protocol for Wireless Sensor Networks**. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/6809875

Yuan, B., Wu, F., & Zheng, Z. (2023). **Post quantum blockchain architecture for internet of things over NTRU lattice**. PLoS ONE, 18(2 February). https://doi.org/10.1371/journal.pone.0279429

Yue, X. et al., (2016). **Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control**. Journal of Medical Systems, 40(10).

Zhang, P., Schmidt, D. C., White, J. & Lenz, G., (2018). **Blockchain Technology Use Cases in Healthcare**. In: P. Raj & G. C. Deka, eds. Advances in Computers. s.l.:Elsevier, pp. 1-41.

Zhang, Y., Tang, Y., Li, C., Zhang, H., & Ahmad, H. (2024). **Post-Quantum Secure Identity-Based Signature Scheme with Lattice Assumption for Internet of Things Networks**. Sensors, 24(13). https://doi.org/10.3390/s24134188

Zhou, L., Wang, L. & Sun, Y., (2018). **MIStore: a Blockchain-Based Medical Insurance Storage System**. Journal of Medical Systems, 42(8).