digital

MDPI

Article

A Regulatory Readiness Assessment Framework for Blockchain Adoption in Healthcare

Olanrewaju Sanda, Michalis Pavlidis and Nikolaos Polatidis *

School of Architecture, Technology and Engineering, Moulsecoomb Campus, University of Brighton, Brighton BN2 4GJ, UK; o.sanda@brighton.ac.uk (O.S.); m.pavlidis@brighton.ac.uk (M.P.)
* Correspondence: n.polatidis@brighton.ac.uk

Abstract: Blockchain is now utilized by a diverse spectrum of applications and is proclaimed as a technological innovation that transforms the way that data are stored. This technology has the potential to transform the healthcare sector, especially the prevalent issues of patient's data-privacy and fragmented healthcare data. However, there is no evidence-based effort to develop a readiness assessment framework for blockchain that combines all the different social and economic factors and involves all stakeholders. Based on a systematic literature review, the proposed framework is applied to Portugal's healthcare sector and its applicability is outlined. The findings in this paper show the unique importance of regulators and the government in achieving a globally acceptable regulatory framework for the adoption of blockchain technology in healthcare and other sectors. The business entities and solution providers are ready to leverage the opportunities of blockchain, but the absence of a widely acceptable regulatory framework that protect stakeholders' interests is slowing down the adoption of blockchain. There are several misconceptions regarding blockchain laws and regulations, which has slowed stakeholder readiness. This paper will be useful as a guideline and knowledge base to reinforce blockchain adoption.

Keywords: blockchain; healthcare; regulatory readiness assessment framework

Citation: Sanda, O.; Pavlidis, M.; Polatidis, N. A Regulatory Readiness Assessment Framework for Blockchain Adoption in Healthcare. *Digital* **2022**, *2*, 65–87. https://doi.org/10.3390/digital2010005

Academic Editors: Mirjana Ivanović, Richard Chbeir and Yannis Manolopoulos

Received: 7 December 2021
Accepted: 9 March 2022
Published: 11 March 2022

1. Introduction

Blockchain has been around for over a decade but has faced regulatory barriers that have slowed its adoption in key sectors. Some of these sectors handle sensitive data and information, such as the healthcare and finance sector [1,2]. Blockchain is, simply put, a distributed database or consensus existing on multiple computers at the same time [3,4]. The longest existing blockchain started in 1995 at the New York Times Newspaper, where the time-stamping service surety was publishing a hash-value in the ad-section of the newspaper every week [5]. There is a widespread misconception that "Bitcoin is Blockchain", which is false. Bitcoin was introduced to the world in 2008 by Satoshi Nakamoto. It is a new form of digital currency called cryptocurrency that facilitates transactions without a central authority [3,6]. The controversy and misconception surrounding Bitcoin is what has led to the issues with regulation and compliance in blockchain technology today [3,7,8].

Despite the advantages of blockchain, the technology is in contrast with existing data-protection laws, which has led to sanctions, lawsuits, and fines in many cases [9]. History has shown that disruptive technologies and the law will eventually find common ground, but this has not yet proved true for blockchain. The year of 2021 marks a milestone for cryptocurrency, as the first Bitcoin ETF was approved in the U.S. in October 2021 [10]. This means that Bitcoin will be traded as a regular investment stock with less volatility [10,11]. This also marks a huge milestone in blockchain regulation, as financial regulators are gradually understanding the opportunities that blockchain technology can provide.

Blockchain technology has seen a rise in adoption in sectors such as supply chain management and manufacturing because of the data and authenticity issues facing these

sectors. There is a call for a legal and regulatory framework to take account of blockchain in sectors that manage the personal information of stakeholders [3,12]. The healthcare sector is overwhelmed with data and multi-level stakeholders. If blockchain is applied to healthcare, it can provide patients and healthcare providers with easy and safe access to medical history. Access to patient data will be provided securely and privately, with the functionality to track authorized access. At present, patient data are fragmented among multiple providers and the web of healthcare systems. Blockchain can offer the patient control of their data in real-time and guarantee data integrity.

Activities, collaborations, and research are ongoing in this area and will eventually see that blockchain is regulated. Cryptocurrency, which is the most popular application of blockchain technology, has not gained much popularity among regulators and big financial houses to date, due to a lack of central control measures, which has left stakeholders exposed. According to Reference [13], hackers have made away with over 2.5 billion USD of cryptocurrency in the last five years. The news of Japan's Coincheck hack of over five hundred ($500) million dollars and Tokyo MtGox Exchange, which lost over 850,000 bitcoins, among others, have made national news headlines [13]. These incidents have given birth to a new wave of regulatory laws that distributed ledger applications have to follow to remain compliant and avoid fines or total shutdown [3,13]. Our review of the regulatory readiness assessment framework for blockchain will guide business entities, solution providers, customers, regulators, and the government on how to develop blockchain-based applications that protect the assets, privacy, and rights of all stakeholders.

In their paper, Gozman et al. [14] proposed a proof-of-concept blockchain system for the regulatory reporting of mortgages in the UK. The benefits of the framework were greater transparency in compliance reporting, a reduction in cost through digitization and a better customer experience. In this paper, we will develop our review based on the lessons learnt from, and discussions on, this prototype. In the future, blockchain may be a solution to data integrity and information-sharing challenges for digital applications. Many business providers and business entities have declared that they are considering leveraging blockchain into their business process. They are aware of blockchain's capabilities but also deterred by regulatory issues in the new technology.

Based on this, we argue that the state-of-art of blockchain regulatory issues have received limited focus. There are some reviews that focus on their application to regulatory reporting; others focus on data enforcement laws on decentralized systems. This has shown a gap for a systematic literature review assessing the regulatory readiness of blockchain adoption and implementation, which was the motivation for this research. Our solution will contribute to the understanding of regulatory issues in blockchain and provides a snapshot of current data laws across some countries. It should be noted that this review cannot be considered all-inclusive as blockchain is growing very fast.

Despite the limited studies on blockchain regulatory frameworks, this paper attempts to answer the following research questions:

RQ1: What are the major regulatory issues of blockchain applications and solutions from a business and technical standpoint?

RQ2: What are the impacts of data laws on blockchain adoption and innovation?

RQ3: How can we examine the regulatory readiness for blockchain in healthcare?

Contributions

There is a growing knowledge repository for the development and adoption of blockchain that will help all stakeholders make more informed decisions [13,15]. The intended benefits of this paper are to reduce the cost of regulatory obligations, accelerate innovation within the blockchain ecosystem and promote collaboration among regulators, business entities, end-users, and solution providers. As a comprehensive study on regulatory readiness for blockchain, this paper makes the following contributions:

- Introduces the regulatory readiness framework research area, presenting a proper foundation, emphasizing definitions, and highlighting terminologies for both industry

and academic affairs. We demonstrate the impact of data laws on blockchain and their enforcement.
- Propose a regulatory readiness assessment framework for blockchain; a framework defining the criteria to assess regulatory readiness and reduce regulatory burdens when adopting blockchain.
- The study is provided in a timely fashion and offers a guiding lamp to strengthen blockchain adoption.
- The proposed framework fills a considerable void in the literature, especially in healthcare, where there is still lack of trust among stakeholders.
- This paper addresses the lack of clarity in blockchain regulatory laws; these issues have become deterrents for stakeholders.
- The proposed framework is adaptable to several sectors and will be of value to policymakers as a tool for assessing readiness for blockchain adoption.

The rest of the paper is as follows: we provide a brief outline of blockchains' architecture and summarize some applications of blockchain in Section 2, followed by the relationship between stakeholders and the proposed framework, in Section 3. We present the application of the framework in Section 4, followed by materials and methods in Section 5. In Section 6, we review the impact of regulatory laws on blockchain adoption. Sections 7 and 8 contain a discussion, the conclusions and future work.

2. Background

In the following paragraphs, we provide a brief overview of the basic architecture and concepts of blockchain. We also offer a summary of some blockchain applications with a focus on regulatory concerns and government impact on blockchain adoption.

Blockchain architecture can be grouped into two categories: private (Permissioned) and public (Permissionless) blockchain [16,17]. Permissionless or public blockchain permits all participants to create a consensus; that is, there is no need for permission to be added as a node on the network [11,16,18]. In this blockchain layout, all participants can read and carry out transactions over the network. A private or permissioned blockchain is when access to participate is granted to only a few on the network [3]. One of the major differences between the public and private is that public blockchains require proof of work or mining, which is used to authenticate transactions [19,20] Another major difference is that, on a private blockchain, all the participants are known, while on a public blockchain, the participants are unknown [16]. A private key is used to sign transactions, while a public key is used to access the transaction. The hash value is encrypted using the private key, and this transaction can be confirmed between two participants on a blockchain network using the public key [16].

The distributed architecture of blockchain means that each block is a reference point to the previous block, which is a hash value from the preceding block, called the Parent Block (as depicted in Figure 1). The block header (Block X) and the block body are composed of the hash value that refers to the previous block. The size of each transaction and size of each block are two very important aspects for maximizing the transactions in a block.

This blockchain layout promotes Confidentiality, Authenticity, and Integrity (CIA) of data and eliminates the risk of both internal and external attacks [19,21]. At present, the major technical drawbacks for blockchain applications are its speed, power usage and scalability [3].

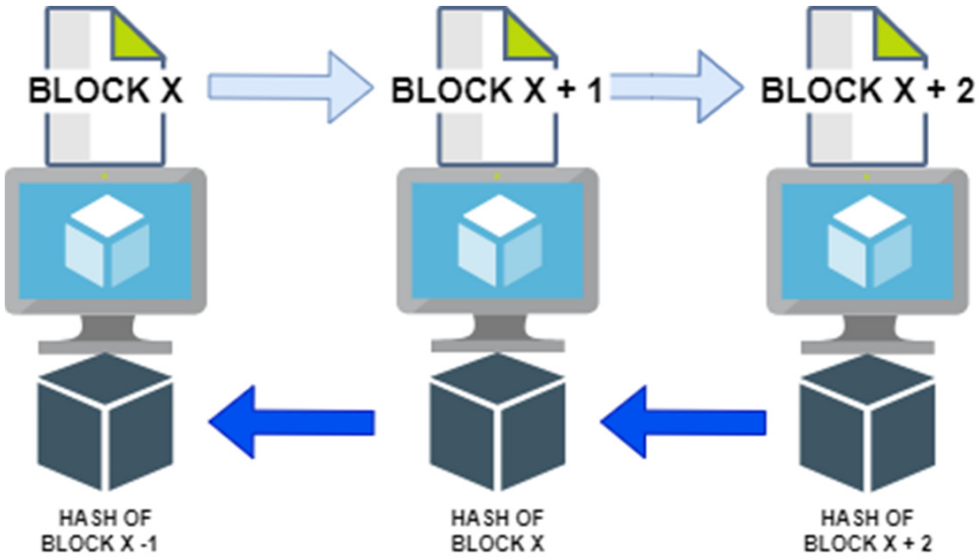

Figure 1. Example of Blockchain Architecture.

Blockchain has shown immense potential to transform the authentication and validation of data assets, but recent studies have emphasized a need for a framework that promotes regulatory compliance [22]. The EU is currently working on a sandbox that brings together regulators, investors, tech experts and companies to test innovative solutions in a controlled environment [22,23]. These solutions will embody the intentional regulations and laws that will be implemented in the pre-coding or pre-design stage of the blockchain application to eliminate bias or undermine traditional regulatory laws [22]. For instance, a blockchain application that is used to provide access to Life Insurance based on the community collectively verifying a person's credit score before the insurance can be approved has a different impact from another that grants approval according to medical and financial history. The first one promotes bias in the community, while the latter encourages socialism [22]. These types of social impacts and issues must be mitigated to create fairness in the use of the technology.

Gozman and Aste, in Reference [14], explored the potential of adopting blockchain technology into regulatory compliance reporting to reduce the burden, cost, and duplication of regulators. They proposed a conceptual blockchain system for the regulatory reporting of UK mortgages. The benefits of this project were a drastic reduction in the cost of regulatory reporting, transparency among all participants, automation of the reporting process and a better end-user experience. Unfortunately, the project did not scale to full implementation, but this created a knowledge pool for financial regulators and businesses to improve on regulatory reporting.

In their article, the Global Systems for Mobile Communications Association (GSMA) [24], propose investment in emerging and disruptive technologies, such as Blockchain, Internet of Things (IOT) and Artificial Intelligence (AI), that have proven to shape the future of companies, allowing them to reach a wider audience and create new integral channels of opportunity. Their report has focused on blockchain as a solution allowing mobile operators, the government, and key stakeholders to work hand-in hand to deliver a better experience in terms of financial services, health, digital identity, and agriculture. The project was a huge success, helping those in rural areas where there is a pressing need for proof of identity. This project faced major drawbacks regarding government regulations. For this project to be a total success, it required some form of government and regulatory approval. This proved to be a challenge because there is no widely accepted regulatory framework that ensures fairness and non-discrimination in the adoption of blockchain. This gave merit to the idea that there is a pressing need for an approved regulatory framework for blockchain that will cut across many sectors.

Esposito, in Reference [16], explored the potential use of blockchain to safeguard medical data hosted in the cloud. The motivation for the research was the increase in data accumulated within the healthcare sector [25]. Their findings showed a growing need for healthcare data to be shared among medical practitioners, for healthcare data to be accessed in real-time by authorized parties, and for these data to be leveraged for a better diagnosis. The current system is a stand-alone Electronic Medical Record (EMR) and lacks interoperability. With new medical smart devices being created, there needs to be a way to accumulate and share these data securely. Their research proposed a blockchain EMR ecosystem, where patient data are stored in a distributed manner, and the patient has control and ownership of their data [16]. This proposed solution was not without its challenges, especially with the data protection laws, such as GDPR, state laws, federal laws, and HIPAA, that exist in the EU and US. Blockchain has not been certified fit to store medical data due to the lack of a regulatory framework within the blockchain ecosystem.

Heston, in Reference [26], conducted a case study in blockchain healthcare innovation to observe how blockchain application can reduce the cost and complexity of managing healthcare records and insurance. The case study focused on the Estonian Government and how they partnered with a private blockchain company called "Guardtime" to create a secure blockchain healthcare record system for its citizens [27]. This innovative approach sprung from a growing population that are unable to pay for their medical bills and an increase in the need for medical care. Heston, in Reference [26], describes how the Estonia government leveraged blockchain to provide a more secure way to share medical data among all necessary participants. The rationale for adopting blockchain technology into the medical sector was the ability to reduce healthcare costs by properly coordinating insurance claims. This new blockchain healthcare initiative was a success, largely because it was supported by Estonia's Health Information System Act of 2007 and the Government Regulation Act of Health Information Exchange in 2008. This has promoted the growth of blockchain in other areas, such as education, tax, and elections, in Estonia. This has put Estonia at the forefront of blockchain adoption in almost every sector of the country. The only challenge faced in the e-health blockchain application was scalability. From these studies, we can extract that the success and failure of a country implementing blockchain into its services not only depends on the layout of the blockchain, but on the data and privacy laws that exist in the country and how the government backs new technologies [26,28]. Therefore, the regulatory readiness assessment for blockchain developed in this research must be in accordance with the data and privacy laws that exist today.

A futuristic approach to the challenges faced by regulators in the EU and US was discussed in their review [29,30]. This research described how public sector services could be revolutionized by a distributed ledger technology. Blockchain regulation has attracted the attention of EU state members, the US Presidency, big financial houses, and big software companies since its exponential growth [30]. The key challenge faced by blockchain adoption stems from the illegal use-cases within the bitcoin community. Some very popular cases involve the money laundering scandal by Liberty Reserve in the US, and the use of bitcoin on shadowy sites and the darknet for malicious purposes. His research proposed a regulatory environment governed by both legal and technical codes to ensure the compliance of blockchain assets. While the EU regulators have adopted a hands-off regulatory approach, the US are focused on regulation after full scalability of the technology; this is not to say that there are no regulations in place [30]. Table 1 provides a summary of the limitations of the studies discussed in the background section. This offers an outline of the research efforts to overcome regulatory barriers in recent years.

Table 1. Summary table of research on blockchain technology.

Citation Number	Authors Name	Year of Publish	Topic	Limitations
[23]	Correia et al.	2021	Evolution of Blockchain Market	Lack of evidence-based studies of regulatory issues associated with blockchain.
[13]	Ekblaw et al.	2016	A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data MedRec: Using Blockchain for Medical Data Access and Permission Management.	Security and scalability of the solution are not discussed.
[16]	Esposito et al.	2018	Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?	The study did not address HIPAA and GDPR laws that guide the use of information technology in healthcare.
[14]	Gozman and Aste	2020	A case study of using blockchain technology in regulatory technology.	The solution was not scaled to production to test its applicability.
[28]	Guardtime	2016	Estonia e-health authority partners with Guardtime to accelerate transparency and auditability in healthcare.	The adaptability and scalability of the solution was not addressed.
[24]	GSMA	2017	Blockchain for Development: Emerging opportunities for Mobile, Identity and Aid.	Regulatory drawbacks have not been considered in detail.
[26]	Heston	2017	A case study in blockchain healthcare innovation.	Lack of applicability to other scenarios.
[22]	Lapointe and Fishbane	2019	The Blockchain Ethical Design Framework. Innovations: Technology, Governance, Globalization.	The research did not go into detail to address the current data laws and how these govern the adoption of blockchain technology.
[29]	Park and Park	2020	Regulation by selective enforcement.	Selective enforcement is difficult to apply in a broader context.
[30]	Yeoh	2017	Regulatory issues in Blockchain Technology.	Their solution requires an approved regulatory framework and standard before implementation can be carried out.

3. The Proposed Readiness Assessment Framework for Blockchain Regulation

In this section of the paper, we propose a readiness assessment framework for blockchain with the key stakeholders and the relationship between each entity. We then introduce some parameters to assess design framework readiness. The key components of this framework have been selected based on the systematic literature review of the blockchain structure and its applications, the key regulatory issues of blockchain, and the stakeholders that will benefit from a regulatory readiness assessment framework for blockchain. The approach to developing this framework is divided into three sections: First, are the facilitating conditions to support blockchain regulation, which involve the creation of regulatory sandboxes, multi-disciplinary research, data protection laws and anonymity. Then, we identify the key stakeholders, which are the regulators and government, business entities, solutions providers, and blockchain end-users [20,27]. In addition, our framework will be based on the dimensions of motivational readiness, structural readiness, engagement readiness and technological readiness, as shown in (Figure 2). Most research done on blockchain, and regulation focuses more on the legal and judicial side of the spectrum; we propose a regulatory readiness assessment framework to test stakeholder readiness for blockchain adoption from a regulatory standpoint. The key stakeholders and their relationships are discussed in the subsections that follow.

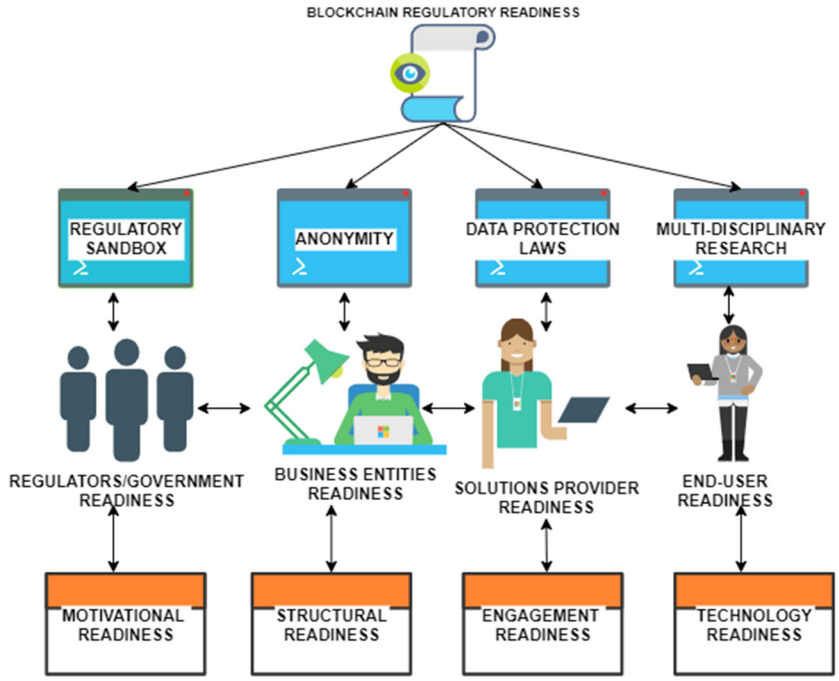

Figure 2. Proposed Regulatory Readiness Assessment Framework.

3.1. Key Stakeholders

3.1.1. Regulators

Regulators can be regarded as the most important blockchain stakeholder because of their direct influence over the blockchain ecosystem. Regulators can determine how easy it will be for other stakeholders to implement blockchain solutions [18]. Regulators are at the forefront of creating legislation and rules-of-engagement for those adopting blockchain solutions.

3.1.2. Business Entities

This refers to the components and processes that make up an organisation. In supply chain management for drug manufacturing, pharmacies, healthcare service providers, research centers and insurance providers will be the business entities that make up the organisation. These will vary according to the blockchain solution that is being adopted and how each business entity will collaborate. Business entities such as healthcare services providers can develop their own blockchain solution or be part of a wider solution.

3.1.3. Solutions Providers

These are the companies that provide the infrastructure need to create blockchain applications and solutions. The number of blockchain solutions providers is gradually increasing, creating healthy competition among these stakeholders. Blockchain solution providers such as IBM and Amazon have continued to show innovation in this space. For example, during the pandemic, IBM launched a blockchain initiative called IBM Rapid Supplier Connect to match frontline workers with essential medical equipment, which was a success.

3.1.4. Blockchain End-Users

These are the direct customers of the blockchain solution. Blockchain has always been a customer-centric solution as opposed to focusing on the organisation. It was created to give the users control over their data and how their data are used. For example, a permissioned or private blockchain solution to manage patient records will give the users control over how their data are shared and stored. The question of who has access and issues of unauthorized access will be reduced.

3.2. Relationship between Stakeholders to Develop a Regulatory Readiness Assessment Framework for Blockchain

3.2.1. Regulators and Business Entities

The adoption of a regulatory readiness assessment framework for blockchain will require extensive collaborative effort between the public sector (regulators) and private sector (business entities). For example, the "RegTech" blockchain prototype was designed to reduce the burden of regulatory compliance and reporting that is placed on organisations. The initiative proposed a decentralized approach for reporting mortgage sales in the UK. This was achieved by a collaborative effort between the Financial Conduct Authority (FCA), which is the public sector, and the banks, which are the private business entities for the success of this project.

3.2.2. Regulators and Solutions Provider

Creating a healthy ecosystem of collaboration and communication between the regulators and the solution providers will improve the implementation of larger projects as well as the scalability of the solution. The Estonian government and regulators have proved the validity of this model through their partnership with 'Guardtime', a blockchain solutions provider [26,28]. This collaborative approach has made Estonia one of the top countries in terms of blockchain adaptability into both public and private services, such as healthcare, finance, and government services.

3.2.3. Regulators and Blockchain End-User

It is important for the government/regulators to work together with blockchain users when creating and regulating blockchain services. This means that regulation will be approached not just from the perspective of solution providers and business entities but from the feedback of end-users. For example, the Estonian government works directly with citizens on the blockchain healthcare system, thereby creating trust and making regulatory compliance easier.

3.2.4. Business Entities and Solutions Providers

A close working relationship between business entities and solutions providers, both large and small, to ensure regulatory compliance and the interoperability of blockchain solutions is key to creating a working framework.

3.2.5. Business Entities and End-Users

There is a need for a direct relationship between business entities and end-users to incentivize users to adopt blockchain technology. Some business entities offer tokens and coins each time a user downloads their blockchain application. This creates trust and better customer relationships. This will also show that the business entities are liable and responsible for their customers' experience.

3.2.6. Solutions Providers and End-Users

This stakeholder relationship is important to protect customers and end-users; it is a key component for the success of blockchain regulation. For instance, in the financial sector, blockchain solutions providers have developed the Know-Your-Customer (KYC) concept to protect users and promote fairness in using the technology. This can be replicated for other sectors and applied in a broader context.

3.3. Regulatory Design Framework Readiness

3.3.1. Motivational Readiness

This refers to the dissatisfaction with the existing or legacy system and the motivation to create a better service for all stakeholders. Motivational readiness is characterised by problem definition, requirement gathering and mapping this to the features offered by blockchain to make it a preferred solution. This creates the catalyst for change in

an organization, for example, a change in healthcare records management due to the duplication and tampering of data. Some examples of the requirements for motivational readiness for blockchain adoption include a need for shared data storage, need for a tamper-proof log of all transactions, automation of business processes, visibility of transactions among all stakeholders, removal of a central authority, and creation of data integrity and trust among stakeholders.

3.3.2. Structural Readiness

Implementing a regulatory readiness assessment framework for blockchain will require expertise, time, money, and resources from organisations. This refers to the workforce and non-technical resources in blockchain adoption. Organisations that are structurally strong in blockchain adoption will be one step closer to implementing a readiness assessment framework into their practices.

3.3.3. Engagement Readiness

This will include, but is not limited to, the ecosystem value proposition, the potential participants, the blockchain ecosystem model, how the ecosystem will be governed, the existing infrastructure and the development costs of the readiness assessment framework. These requirements will be mapped to other components of the framework to promote collaboration.

3.3.4. Technology Readiness

This refers to the technological infrastructure that is currently in place and the required information and communication resources for blockchain adoption. Embracing and complying with blockchain regulation and adopting a regulatory readiness assessment framework will require access to certain levels of technology. Some examples of technological readiness include cloud storage, computers, smart phone, and mobile connectivity.

4. Application of Framework in Case Study

In this section of the paper, we introduce the application of the proposed framework and demonstrate its applicability using Portugal's healthcare sector (Appendix A). The Portuguese healthcare sector has grown significantly and was ranked as the 13th best in Europe [31]. The Portuguese government is pushing for patient rights and secure access to information. They are considering blockchain as an innovative solution to address this problem.

4.1. Regulatory/Government Readiness

The Portuguese government/regulators are the most important stakeholders when creating an acceptable regulatory framework for blockchain. Since the global COVID-19 pandemic, the Portuguese government has been slow in their adoption of blockchain into sector specific services, unlike other EU countries, such as Malta and the UK [23,32].

There have been some improvement since the publication of the digital transition action plan, in April 2020, in preparation for the regulations on and legislation of digital technologies [33]. Since then, there has been significant blockchain research in the energy, smart contracts, health, and Non-Fungible Tokens (NFT) sectors [34]. Most of the research into adopting blockchain into healthcare in Portugal is still at the inception stage. This will prove to be a complexity in getting the stakeholders in our case study to accept a blockchain solution, and the lack of regulatory framework in this sector is one of the major deterrents.

This validates the need for a blockchain regulatory readiness in the areas of technology and structural readiness, but points to a lack of motivational and engagement readiness in the Portuguese healthcare sector. Our regulatory readiness assessment framework can assist the government in creating a widely acceptable regulatory framework for blockchain technology by identifying the readiness of key stakeholders and mapping them to the key facilitating conditions that can promote blockchain regulatory and knowledge. This

can be designed into a template to promote blockchain innovation and bridge the gap with legislation.

4.2. Business Entity Readiness

From our findings, we outlined a slow growth into blockchain research among many small and large companies in Portugal. This highlights the fact that most are familiar with the term "Bitcoin" but unfamiliar with the term "Blockchain" [35]. The foreign interest in the Portuguese blockchain market has grown since the release of the government's publication regarding the creation of Technology-Free Zones [23]. This created anticipation that, when the TFZ legislative framework is created, it will create a more stable platform for blockchain solutions. Some of the most successful use-case areas of blockchain in Portugal are in Ethereum, charity and gaming. There are considerable limitations from a structural and technological perspective. Therefore, the readiness for a regulatory framework for blockchain solution within business entities is very high, but motivational and engagement readiness is very low.

4.3. Solutions Providers Readiness

Information from the relevant literature on the current state of blockchain technology in Portugal show that many blockchain consulting firms have already been established with a firm foundation. From our findings, we can point to a readiness for solution providers in our four dimensions. Technology, motivation, structure, and engagement readiness are relatively high. This can create a solid foundation for a nationwide, accepted regulatory framework and practice when creating blockchain solutions. Our regulatory readiness assessment framework can assist solution providers in gauging readiness to achieve regulatory compliance when implementing blockchain solutions. Solution providers are focusing more on blockchain in the financial sector because Portugal is tax-free for cryptocurrency [35]. The successful implementation of blockchain into healthcare in Portugal has yet to be achieved, but this may change after the COVID-19 pandemic due to the pressure on the healthcare sector to share and manage a high volume of information.

4.4. End-User Readiness

There is high motivation for a new way of managing healthcare records among patients (end-users) in Portugal; this shows a decent motivation to extend blockchain to the healthcare sector [31,36]. This will have to be achieved in compliance with EU data laws, which is where our regulatory readiness framework can be applied. From our findings in recent studies, there is a growing concern regarding patient autonomy over their data in Portugal. As with the issue of the data breach in our case study, there is news of several other hacks into medical record and breaches into solution providers [11,21]. We highlight strong evidence of engagement, motivation, structural and technology readiness for a healthcare record blockchain solution.

The stakeholder readiness and their corresponding regulatory facilitating conditions were explored by applying our regulatory readiness framework to the case study in Portugal. This showed readiness for a widely acceptable blockchain regulatory framework to boost innovation in the blockchain space in Portugal [31,33,34]. The motivational and engagement readiness for regulators and business entities is *low,* while that of the solution providers and end-users is *high*. On the other hand, the structural and technological readiness for all key stakeholders is *high*.

The key facilitating conditions for regulators to achieve regulatory readiness will include *regulatory sandbox* and *data protection laws,* while the business entities and solution providers will be facilitated by regulatory sandbox, anonymity, and data protection laws. Finally, the key facilitating conditions for end-users will be anonymity and data protection laws.

4.5. Applying Key Regulatory Facilitating Conditions to Stakeholder Readiness

4.5.1. Regulatory Sandbox

A regulatory sandbox will allow innovators and researchers to test out new technology and business models without the rules and consequences of the real world. Most of the discussion concerning blockchain is centered around bitcoin, and we clarified, earlier in our research, that Bitcoin is not Blockchain. There is still no clear regulatory framework for blockchain in Portugal, especially for the healthcare sector. Therefore, we propose a regulatory sandbox among regulators/government, business entities and solutions providers. A regulatory sandbox will allow for the testing of new innovative blockchain solutions within a controlled environment. This will contribute to the knowledge sharing of data laws and provide evidence on blockchain regulatory issues and how key stakeholders can harmonize legislation and blockchain solutions.

4.5.2. Anonymity

For blockchain solutions, especially in healthcare and finance, there is a need to balance the anonymity of blockchain assets with anti-money-laundering laws, KYC and GDPR laws. Defining this clearly from the design to the implementation stage will have huge impact on a globally accepted regulatory framework. This is one of the major facilitating conditions that will harmonize legislation and blockchain technology in Portugal and can be applied in a broader context in other countries. Anonymity is considered a key facilitating condition for business entities, solutions providers, and end-users. There are technologies in place, such as zero knowledge (zk-SNARks) and ring signature, that can be used to hide the identity of the transaction sender on the network. Encryption can also be used to protect the user's privacy.

4.5.3. Data Protection Laws

For Portugal, this falls under the category of enhanced privacy and trust in data. There is a big push for a more effective data-management platform, especially in the country's healthcare sector [23]. The government is discussing initiatives to secure patients' rights regarding how their data are shared and accessed among healthcare practitioners. Understanding the current data protections laws, such as the GDPR "right to be forgotten" and implementing these across the blockchain ecosystem will reinforce the confidence of stakeholders. This key regulatory facilitating condition will be important to regulators, end-users, business entities and solution providers.

4.5.4. Multi-Disciplinary Research

This is one of the most important components of the framework. This promotes engagement readiness among all stakeholders, irrespective of academic background and discipline. It is the catalyst to achieving an industry/sector-wide regulatory framework for blockchain and its assets. The process of multi-disciplinary research will require a collaborative approach among several countries, sectors, disciplines, and businesses that indirectly or directly influence blockchain regulation. This is quite different from the regulatory sandbox and promotes stakeholder engagement at a high level by exploring new opportunities and ideas. Each person or entity will provide a unique and diverse set of skills and knowledge that will add to the knowledge pool of blockchain and how to achieve effective regulation that will not harm innovation efforts. For example, multidisciplinary research into blockchain regulation will involve the legal sector, business sector, the social-science sector, computer science, healthcare, economics and technical and non-technical blockchain experts.

5. Materials and Methods

The search for relevant papers for the Systematic Literature Review was carried out using the Scopus Database. This is a concise database that encompasses a wide array of journal articles, so the enquiry was limited to this search engine. The goal was to retrieve

the literature directly relating to blockchain regulations and blockchain in healthcare records' management. The keyword used for the initial search was "Blockchain", with the inclusion criteria for "business & management studies", "Computer Science" and "Healthcare". Conference papers, conference reviews, book chapters and unpublished works were excluded. After removing duplicates and categorizing the literature based on these inclusion criteria, our initial search provided 25,680 articles on blockchain. Following further title-, abstract- and keyword-screening for studies that focus on regulatory concerns of blockchain in healthcare, blockchain regulation and regulatory impacts on blockchain, we shortlisted our list of articles to 135. Highly technical studies, such as blockchain analytics and algorithms, were excluded from the search. After further consideration and review, we selected 23 articles for the review. Figure 3 shows a flowchart of the literature search and selection criteria.

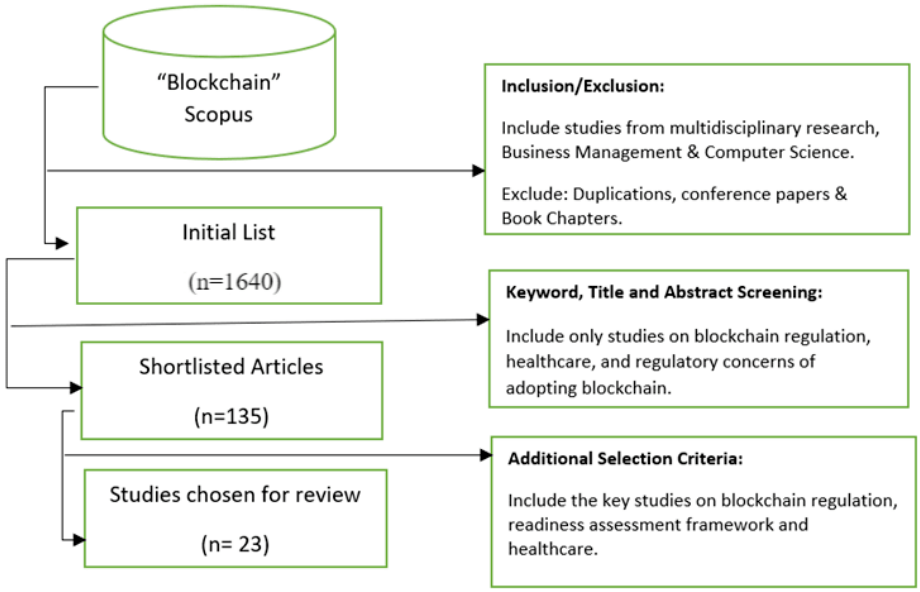

Figure 3. Systematic Review of Blockchain Regulation and Adoption.

Our review of the chosen literature revealed gaps in blockchain regulation research and its adoption within the healthcare space and other sectors. We present a summary table of the chosen studies (as shown in Table 2). Attempts to gain primary data on blockchain regulatory frameworks were limited but it a growing area. Most research studies showed a lack of understanding of key facilitating conditions for blockchain regulation. Despite these gaps and after a careful synthesis of studies, we were able to:

- Gain more knowledge and understand the various applications of blockchain.
- Understand the implications of regulations and data laws on blockchain.
- Understand the roles of the key stakeholders associated with blockchain regulation in the healthcare sector.
- Understand their concerns regarding regulation, privacy, and security.

This systematic literature review provides the conceptual and theoretical foundation for our proposed regulatory readiness assessment framework. While we accept that there is no single framework that is sufficient to assess the regulatory readiness of a sector or country to adopt blockchain, we combined all effort and knowledge to ensure the reproducibility of the proposed framework [37]. We addressed the limitations of blockchain from a technical, economic, and social perspective, then carefully applied this to our proposed framework. We successfully identified the key stakeholders that can promote or limit blockchain regulation, which is very important to ensure that blockchain can gain the popularity required for proper regulation.

Table 2. Summary of the important literature for blockchain regulation and adoption in healthcare and other sectors.

Study/Summary	Methodology	Key Stakeholders
Belchior et al. (2021) [6] Summary: A framework for blockchain interoperability among blockchain entities. Benefits: Reducing attacks through interoperability; improving data standards and privacy; insight into blockchain interoperability use-cases. Challenges: Fast-paced development of blockchain, security, trust and privacy issues related to GDPR.	Systematic Literature Review	Business Entities Regulators Service Providers
Berdik et al. (2021) [18] Summary: Reports on the issues and adoption of blockchain applications in information systems. Benefits: Promotes blockchain adoption and interoperability among components; open source blockchain tools. Challenges The layout and architecture of blockchain is crucial to its widespread adoption.	Secondary Sources (Survey)	End-Users Solutions Providers
Casino et al. (2019) [38] Summary: The use of blockchain in supply chains, healthcare, IOT and data management. Benefits: It contributes to the knowledge base and understanding of applying blockchains to real-world problems. Challenges: Lack of review of current state-of-the-art devices due to limited information and research.	Literature Review	Blockchain Researchers Regulators Business Entities
Charles et al. (2019) [7] Summary: Explores the use of blockchain-based application for clinical research, managing patient and laboratory data. Benefits: Contributes to the knowledge and understanding of the regulatory constraints of adopting blockchain into the healthcare sector. Challenges: Adhering to regulatory requirements, privacy regulations and guideline on how to achieve compliance when managing healthcare records.	Secondary Sources	Patients Regulators/Government Healthcare Providers Solutions Providers
Dameri (2009) [9] Summary: How to improve IT governance and compliance of digital applications. Compliance requirements when implementing IT governance into digital applications. Benefits: Development of a compliance-automated system. Challenges: Transparency, costs, data protection laws.	Secondary Sources	Solutions Providers Regulators/Government
Dorri et al. (2017) [19] Summary: An investigation into the use of blockchain in a smart-home setting. Benefits: Proposed a blockchain smart-home framework that is secure, and secure access control for IOT devices. Challenges: Confidentiality, high costs and security issues.	Experiment	Solutions Provider Blockchain Developers
Ekblaw et al. (2016) [13] Summary: Proposed the use of blockchain to manage medical records. Benefits: The development of a working prototype to analyse the potential of blockchain in healthcare, improved interoperability of systems among healthcare providers and quality data for medical researchers. Challenges: 51% attack on the private blockchain, high volume of medical data.	Case Study (Experiment)	Patients Healthcare Providers Regulators Public Health Authorities.
Esposito (2018) [16] Summary: Proposed a blockchain solution to protect healthcare data hosted within the cloud. Benefits: Recommends off-chain storage to combat GDPR "Right to be forgotten' law. Challenges: GDPR Laws, scalability, and storage of data.	Secondary Sources	Patients Healthcare Providers Regulators Solutions Providers

Table 2. *Cont.*

Study/Summary	Methodology	Key Stakeholders
Filippi and Hassan (2016) [39] Summary: An overview into the legal challenges of blockchain applications. Benefits: Proposed automated legal governance using blockchain, improved transparency in carrying out regulatory obligations. Challenges: Issues with GDPR's right to be forgotten and immutability of blockchain transactions.	Secondary sources	Regulators Law Makers Business Entities
Gozman et al. (2020) [14] Summary: Automating the process of regulatory reporting using blockchain technology. Benefits: Reduce duplication, efficient regulatory reporting system, and creating a better understanding of blockchain for regulators by making them use the technology in regulatory reporting. Challenges: Educating regulators and other stakeholders, confidentiality issues.	Secondary Sources	Regulators/Government Financial Houses Business Entities
Gupta and Sadoghi (2019) [40] Summary: Proposed the use of blockchain in processing transactions. Benefits: Improves trust and data integrity, tamper-proof solution, reduce fraud and accountability of data. Challenges: High costs of maintenance and regulatory issues.	Secondary Sources	Business Entities Solutions Providers
Heston (2017) [26] Summary: The application of blockchain in healthcare innovation using Estonia as a case study. Benefits: Promotes better understanding of regulators, governments, and healthcare providers on the use of blockchain in the healthcare sector and how to leverage the opportunities provided by blockchain to improve healthcare data integrity. Puts the patient's welfare at the forefront of innovation. Challenges: 51% attack can occur; size of medical data can cause storage problems and end-user is responsible for data.	Case Study	Patients Regulators/Government Healthcare Providers Business Entities
Kwok and Koh (2018) [4] Summary: Explores the use of blockchain to boost tourism among small economies. Benefits: Increased commercial opportunities for small countries and improved stakeholder knowledge on blockchain. Challenges: Educating stakeholders on blockchain and regulatory gaps.	Secondary Sources	End-users Business Entities Regulators/Government
Lim et al. (2021) [36] Summary: How blockchain technology can be used to improve supply chain activities. Benefits: Improve stakeholder knowledge of using blockchain in supply chain tracking and management. Challenges: Transparency, high costs and lack of expertise.	Literature Review	Solutions Providers Business Entities
Lin et al. (2017) [12] Summary: The security issues and challenges of blockchain, and how these have shaped regulation laws and the adoption of blockchain as a solution. Benefits: Easy access to data, integration of multiple tasks and less maintenance. Challenges: Privacy issues.	Secondary Sources	Regulators Solutions Providers
Kwok (2018) [41] Summary: This research focused on the adoption of blockchain technology into Tourism and the implications for tourism development in the Caribbean economy. Benefits: Boosting of tourism revenue and the launching of the first digital legal tender in the Caribbean. Challenges: Lack of IT infrastructure and government support for new technologies.	Survey	End-users Government Business Entities

Table 2. *Cont.*

Study/Summary	Methodology	Key Stakeholders
Nguyen et al. (2021) [32] Summary: An extensive survey into the application of blockchain and AI into combating the COVID-19 virus. An integration of blockchain and AI to revolutionize the healthcare sector. Benefits: Early detection of outbreaks, ordering of medical data, support drug manufacturing and virus tracing. Challenges: Lack of a regulatory framework for blockchain, data privacy concerns, implementation issues and interoperability of medical record systems.	Survey	Patients Government Healthcare Providers
Prashanth (2018) [21] Summary: A survey into the challenges and opportunities of using blockchain as a solution to privacy concerns. Benefits: Improves trust in and credibility of data and has no third parties. Challenges: Fear of strict regulations.	Secondary Sources	Solutions Providers Business Entities
Sarmah (2018) [2] Summary: A study into understanding the use of blockchain and how to it can be applied to several industries and sectors, as well as their challenges and advantages. Benefits: Promotes a better understanding of how to leverage blockchain as a solution for organisations. Challenges: A lack of regulatory framework is slowing down the pace of adoption and a lack of understanding of blockchain architecture by the key stakeholders.	Secondary Sources	Solutions Providers Regulators
Siyal (2019) [42] Summary: An overview into blockchain application in the healthcare sector, focusing on Electronic Health Records, clinical research, medical fraud detection, neuroscience, and biomedical research. Benefits: New research opportunities for biomedical research. Challenges: Storage and scalability, requires regulatory standards, social acceptance, and interoperability of healthcare systems.	Secondary Sources	Healthcare providers Biomedical researchers R&D Specialist Patients Solutions Providers
Yeoh (2017) [30] Summary: This research examines the key regulatory challenges of blockchain adoption in the EU and US. It discusses the hands-off approach initiated by both countries, and how this has accelerated the growth of blockchain, in detail. Benefits: Support for the right innovation for blockchain that will continue to add value to the technology and make it more accessible. It also promotes a better understanding between cryptocurrency and blockchain. Challenges: Lack of adequate knowledge and blockchain expertise from regulators.	Primary Sources Secondary sources	Regulators Governments Solutions Providers
Kant (2021) [43] Summary: Blockchain as a solution to organisations' needs and a source of competitive advantage. Benefits: Contributes to the body of knowledge of blockchain adoption. Challenges: Social and legal issues.	Secondary Sources	Blockchain Researchers Solutions Providers
Pal (2021) [44] Summary: Explores the possibility of applying blockchain to business management and business activities to create a safer transaction process. Benefits: Safer business transactions, reduces error in transactions, helps prevent fraud. Challenges: Regulatory and social challenges.	Systematic Literature Review	Business Entities Solution Providers Blockchain Researchers

Table 2. *Cont.*

Study/Summary	Methodology	Key Stakeholders
Rajeb (2020) [45] Summary: Explores the application of blockchain to food supply chains (FSC) to combat the issue of food traceability, improve health and safety standards of food, provide verifiable information on food nutrients. Benefits: Improve supply chain transparency, effective traceability, automate data collection and minimize logistic errors. Challenges: Limited scalability, technological immaturity, lack of industry standard, lack of a blockchain regulatory framework and privacy concerns.	Systematic Literature Review Bibliometric Analysis.	Food Manufacturers Food Regulators Business Entities End-Users
Sung (2021) [46] Summary: This study focuses on the adoption of blockchain in an identity management system, with a focus on the Korean Government. Benefits: Blockchain provides better control of data, integrity and data reliability and reduces the cost of delivery to public services. This system is a user-centric personal data management without a central authority. This will allow for quicker data access by leveraging the decentralized nature of blockchain. Challenges: Educating public sector on blockchain, privacy concerns, regulatory concerns.	Design Case Literature Review	End-users Government Regulators Public Sector

Some of the studies, such as Casino et al., Charles et al., Dameri, Dorri et al., Gupta and Sadoghi, Kwok and Koh, Lim et al., Sarmah, Siyal, Kant, Pal and Sung, proposed different methods for blockchain adoption and highlighted some related and non-related regulatory issues pertaining to blockchain. The primary components of the framework were chosen from framework- and regulatory-related studies on blockchain (Belchior et al., Berdik et al., Ekblaw et al., Esposito., Filippi and Hassan, Gozman et al., Heston, Lin et al., Nguyen et al., Prashanth, Yeoh and Rajeb). Most of these reviews and studies were limited in scope but offered a good theoretical foundation for the proposed framework. Most reviews focused on one aspect of organisations and stakeholders, while ours considers different levels of stakeholder readiness. Defining the stakeholders responsible for adopting new technology is very important to the framework, especially for a multi-stakeholder sector such as healthcare.

6. Impact of Regulatory Laws on Blockchain Adoption

Blockchain-enabled applications are currently fighting the battle of compliance and how to navigate the parameters of data privacy laws such as GDPR, Health Insurance Portability and Accountability Act (HIPAA), SEC, California Consumer Privacy Act (CCPA), tax laws, state laws, anti-money-laundering laws, and anti-corruption laws [8,35,47]. Policymakers and business entities will have to collaborate on the laws and rules of engagement that surround blockchain for innovation to continue at a fast pace [9,38]. This proposes the question of whether the existing laws will be modified to suit blockchain or whether there will be entirely new set of rules for blockchain assets [40].

Blockchain is built on transparency, trust, and immutability; therefore, many sectors are adopting it into their business process. This unique characteristic is also the reason it is facing resistance from regulators [4,5]. Blockchain has been envisioned to become a new tool of democracy, giving control over personal data back to the users, as well as the power to monetize their data [7,38,40]. The lack of compliance, governance, and adequate regulations in blockchain technology is slowing down its adoption and innovation in several sectors and industries [8,35]. This is one of the major challenges faced by emerging technologies such as Artificial Intelligence (AI), Internet of Things (IOT), 3D Printing and Virtual Reality (VR) [48].

Blockchain is a catalyst for change and will eventually blend with regulation and legislation [3,28]. The impact of data laws and regulations on blockchain applications is no longer passive. The EU, according to GDPR laws, has rules and regulations regarding

how data are managed and transmitted; these are enforced across all traditional digital assets. For instance, the GDPR Regulation (2016/679) of the European parliament and Council protects the processing of personal information and the free movement of such data [49]. This creates an issue in the world of blockchain technology due to its special characteristics, such as the anonymity/pseudonymity, immutability, and distributed nature of this innovative technology [7,15,41]. The decentralized structure of blockchain violates the first rule of the GDPR, which is the "Right to be Forgotten"; this is the right for an individual to request that their personal data are removed or erased, which is impossible on a blockchain ledger [49].

According to Siegel [50], the HIPAA laws consist of two major categories: the HIPAA Privacy Rule and the HIPAA Security Rule. The HIPPA Privacy rule is a collection of national standards for the protection of certain patient information, while the HIPAA Security Rule is a collection of security standards for patient information that is transferred or exchanged in the US [50]. The current HIPAA laws are in direct contention with blockchain because encryption or cryptography is in direct violation of HIPPA privacy and security rules. This is a challenge when proposing solutions using blockchain to the authentication and verification of medical data in the US. Companies such as Timcoin are currently working on blockchain uses in the healthcare industry that can navigate the HIPAA rules [33,50].

There are also laws such as state laws, tax laws and anti-corruption laws that vary from country to country. Blockchain companies must consider these laws according to where data will be stored and transmitted, who will have access to data, and the purpose of the blockchain [35].

6.1. Key Issues between Blockchain and Current Data Protection Laws

At present, digital applications operate using a central or single database that serves as a single source of truth [16,35]. This master database can easily be shared with regulators and authorities for enforcement and investigations. Blockchain, on the other hand, operates as a distribution of nodes and acts as a consensus version of the truth [47]. This has made regulation complex because it is difficult to ascertain ownership of the network in a decentralized network. Blockchain is characterized by anonymity and pseudonymity, making it difficult for enforcement agencies and police to enforce laws [39,50,51]. Blockchain is an immutable ledger, which means that transactions cannot be deleted once they are entered [41,52]. This creates another dilemma with regulatory laws and regulators due to data privacy laws. These are some of the major gaps that exist between enterprise blockchain and regulation.

There are some major key legal hurdles that blockchain companies must overcome to comply with data laws and regulations. Some of these hurdles are due to the technical features of blockchain, while others are based on territory. They are as follows.

6.1.1. Recognizing Blockchain-Based Signatures

On a blockchain ledger, it is easy to know who owns the stored data and prove that data have not been manipulated by users. According to the regulators, this is insufficient, as they are not legally binding. For blockchain-based signatures to be legally binding, regulators will need to know who made the transactions, the time stamp, who validated the transactions, the data associated with the transaction, and was it carried out under a trusted Internet Service Provider (ISP) [31,51]. To mitigate these legal hurdles, regulators will be required to broaden their knowledge of blockchain timestamping methods and how this can fit into the current regulations [35].

6.1.2. Location of Nodes

Permissionless or public blockchains such as Bitcoin are not hosted in one precise location, but a combination of nodes that are spread out across the globe [41]. This can make it difficult for regulators, especially in the finance sector, where there are anti-money-

laundering laws and know-your-customer (KYC) laws. This will require a cross-jurisdiction effort on the part of regulators to comply with data laws. There is also the drawback of being unable to control risks and monopolies that exist in the blockchain ecosystem. EU regulators focus on the location of a dispute to determine the appropriate laws that will govern damage recovery [31]. The place where the harmful event or hacking occurs usually determines which court will have jurisdiction. The decentralized structure of blockchain will make it difficult to determine in which place or country the damage occurred and will make it hard for the law to take its course.

6.1.3. Anonymity

When a law is broken, law enforcement does their job by enforcing sanctions and penalties. For this to happen, the law will have a clear idea of who the lawbreakers are and where they reside. For blockchain, this is quite impossible or very difficult to ascertain. For permissioned or consortium blockchains, this will not be a problem because all participants are identified, but for a permissionless blockchain, where the actors are unknown, this can be quite difficult and will require forensic analysis of the blockchain network [32]. To mitigate this issue in Bitcoin, for instance, the regulators will need to police the gateway between cryptocurrency and fiat currency [34,35]. Regulators will be able to monitor the access points that are key to the running of the blockchain application. By policing these access points, lawbreakers can be unmasked and traced.

6.1.4. Liability Constraints

Who is liable? The question of who will be liable and responsible for data breaches or violating data laws can be confusing in blockchain. This lack of liability can create an obstacle for regulators to establish with compensation rights for defrauded users [34,53]. The issue of who is most liable among blockchain developers, users, and business entities is still under debate, so the government has decided to find a different way of enforcing liability in blockchains [32,34].

6.1.5. Data Protection Laws

The EU has enforced GDPR rules since 2018, whose sole purpose is to consider all developments in the online world for the last 25 years [49,51]. The GDPR laws were designed before the popularity of blockchain grew to its present levels. This has created tension between blockchain technology and EU data regulators. There are three major areas of contention between blockchain and GDPR laws, which are as follows:

- The identification of data controllers and processors is law under GDPR.
- Anonymity of personal data.
- The GDPR right to be forgotten.

The third contention, which is the "Right to be Forgotten", can be mitigated if the blockchain is designed with this data law in mind [50]. The use of an off-chain storage and processing data management platform can mitigate this issue.

6.2. Some Key Guidelines to Aid Regulators and Policy Makers on Their Journey to Regulate Blockchain Technology

- A simple dictionary of blockchain terminologies written by regulators, which defines blockchain EU Laws and data laws to ensure shared definitions among countries.
- Communication of these terminologies so that they reach a wider audience.
- Creation of a balance between blockchain terminologies and laws that will not deter innovation.
- A sandbox to improve understanding between regulators and the blockchain ecosystem.
- Use of case testing to obtain a clearer picture of the gap between blockchain and GDPR.
- Monitoring and reiteration in smaller use cases to test resistance to blockchain assets.

- A based regulatory tool is a good way of improving the understanding between regulators and blockchain. In their work Gozman and Aste [14] proposed a solution that involved the application of blockchain to regulatory reporting. This will help bridge the gap and harmonize the current situation between the data-protection regulators and blockchain solutions as they utilize this technology first-hand.

7. Discussion

The authenticity of a framework is ascertained when its explanations are concise, categories are properly formed, interpretations and terminology are easy to understand, and transferability and dependability are established [47]. We present a summary of the regulatory readiness assessment framework for the Portuguese healthcare sector, as shown in Table 3. We provide a snapshot of the findings based on the key regulatory facilitating conditions, which is key to the framework. We categorize facilitating conditions from '*high*' to '*low*' based on key stakeholder readiness. We capture how the key regulatory facilitating conditions influence stakeholders and highlight their readiness for a regulatory framework for blockchain technology. These findings are based on our Portuguese healthcare case study.

Table 3. Summary of the regulatory readiness assessment framework for Portugal's Healthcare Sector (case study) in terms of key regulatory facilitating conditions.

Key Regulatory Facilitating Conditions	Regulators/Government	Business Entities	Solutions Providers	End Users
Regulatory Sandbox	**Low** There are plans to launch a Trade-Free Zone in Portugal, but there is no ongoing collaborative approach between regulators and blockchain providers. There is a need for a regulatory sandbox to improve the understanding of regulators in Portugal that Bitcoin is not Blockchain.	**Low** There is little to no collaborative effort among business entities to improve blockchain adoption and minimize regulatory concerns.	**High** There are collaborative research plans among the bigger technology companies to reduce regulation concerns by following regulatory practices when providing their blockchain solution.	**High** High stakeholder motivation for blockchain adoption and innovation, especially due to Portugal's tax-free law on cryptocurrency, but fear of harsh regulation causes concern.
Anonymity	**Low** Regulators and government understanding of blockchain anonymity is based on the darknet uses of Bitcoin. Regulators must have a technical understanding that blockchain anonymity is not a threat but an opportunity if leveraged correctly. There are always ways to reduce anonymity within a technology, but only through an understanding of its technology and terminology.	**High** Business entities are individually taking advantage of blockchain in Portugal, especially cryptocurrency, which is the most popular use-case at present.	**High** Solution providers such as Amazon and IBM are trying to figure out ways to blend anonymity when developing blockchain platforms with regulatory requirements.	**Low** There are concerns regarding how issues will be resolved and the high risk of losing their investments if everyone is anonymous.
Data Protection Laws	**High** The EU is considering blockchain regulation despite most laws still being at the planning phase.	**Low** Concerns relating to GDPR data laws and fines.	**Low** Concerns relating to GDPR laws, Portuguese data laws and anti-money-laundering laws.	**Low** Concerns relating to laws of the regulatory framework and how these will impact their data.
Multi-Disciplinary Research	**High** There is motivation for research on blockchain regulation to cut across all sectors, even though most research is still in the planning phase. There is also a good IT infrastructure in Portugal.	**Low** There is no known multi-disciplinary research on blockchain regulation among business entities in Portugal.	**Low** There is limited multi-disciplinary research among small and large solution providers.	**High** End-users show motivation to be part of multi-disciplinary research that forms a knowledge pool for the creation of a regulatory framework.

One of the key results is that all stakeholders need to understand the technology and terminologies, which will require extensive collaboration. Most blockchain initiatives have faced challenges in gathering all stakeholders together to discuss a roadmap for a widely

acceptable regulatory framework. The key concern of most business entities and end-users relates to data protection laws. Addressing these concerns by creating a regulatory sandbox to test blockchain solutions in a controlled environment will boost blockchain's adoption into the healthcare sector and other industries.

There is strong evidence of blockchain adoption and innovation in Portugal. This willingness to adopt blockchain as a solution provides the correct ecosystem for a widely approved framework that supports innovation. The fault tolerance of the proposed solution is synonymous with distributed systems. By design, the proposed readiness assessment framework will maintain its functionalities if one or more of the components fail due to their unexpected behaviors. The issue of scalability will heavily depend on the number of stakeholders that are involved in the process and the transactions of the blockchain application. There is a need for a regulatory readiness framework that will address the concerns of all stakeholders without comprising the innovative potential of blockchain technology.

8. Conclusions and Future Work

The blockchain phenomenon has now moved from an exaggeration to a reality. This innovative technology is gradually disrupting the digital ecosystem and has the power to transform not only the financial industry, but almost every industry and sector in the world. There is ongoing research and collaborative efforts toward regulating this technology but no evidence of any research into the regulatory readiness assessment for blockchain technology. In this study, we proposed a conceptual regulatory readiness assessment framework for blockchain. This was then applied to the Portuguese healthcare case study to test its usefulness. We identified the key stakeholders that are needed to achieve a regulatory framework, the technology, motivational, engagement and structural readiness, and the key regulatory facilitating conditions for blockchain. This gave a good insight to the application of blockchain to manage healthcare records, with Portugal as a focus point for our case study. Our findings showed positivity regarding the adoption of blockchain, especially in the healthcare sector, where patients want full control over their data, there are issues of fragmented data, and healthcare providers require data integrity. The downside in our findings points to a lack of harmony between regulators and blockchain stakeholders due to the lack of a dependable regulatory framework. Applying a regulatory readiness framework to blockchain will speed up its adoption, guarantee knowledge dissemination, reduce loss of data, avoid fines, and improve regulatory reporting. Blockchain development and regulatory compliance will be approached simultaneously at every level of the framework, with the key stakeholders as variables.

Blockchain can enhance data integrity in many sectors especially healthcare but there must be trust between the technology providers, regulators/government, business entities and end-users. Much is still unknown about blockchain regulation at this stage and, as it grows from strength to strength, regulation will become mandatory. This will have to be done on a use-case-by-use-case basis, rather than using one-size-fits all approach. Although our framework was based on a wide view of blockchain in terms of its regulation, adoption, and innovation, it does not cover every aspect of blockchain regulation.

For future research, we propose research into a web application tool for blockchain adoption and a regulatory readiness assessment. This will be conducted using a collaborative approach with a wider number of researchers, with a focus on its application in the healthcare sector. The healthcare sector is slow to accept digital transformation and has limited information when it comes to blockchain application. Despite these limitations, we believe that our regulatory readiness assessment framework will improve regulatory knowledge for the use of blockchain in healthcare and other sectors.

Author Contributions: Conceptualization, O.S., M.P. and N.P.; methodology, O.S.; validation, M.P. and N.P.; writing—original draft preparation, O.S.; writing—review and editing, M.P. and N.P.; supervision, M.P. and N.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Appendix A. Case Study Brief

We selected a hospital in Portugal that was fined for GDPR infringement and violating data regulatory laws for our case study. After evaluating several pieces of secondary data (research journals and articles) on regulation in the EU, we chose Portugal because of its recent effort towards blockchain adoption and nation-wide regulation. A case study approach seems appropriate because of the limited information regarding blockchain adoption and regulatory research in the healthcare sector. We have looked through extensive news coverage and information on this case study to obtain a comprehensive understanding, and most of the data were compiled from secondary data sources. We focused on secondary data that showed the anticipated challenges regarding blockchain in Portugal, the current state of regulation, and stakeholder readiness for blockchain technology. We used secondary data corresponding to our themes, which were the key facilitating conditions for blockchain, identification of relevant stake holders and stakeholder readiness, when selecting our case study.

From our findings, we identified several news headlines about the 400,000 EUR fine slammed on the hospital for violating data laws, which was the first of its kind [34]. The Portuguese-based hospital was accused of violating three EU data laws, as follows: indiscriminate access to patient's data, lack of secure processing, and violation of confidentiality and integrity. The hospital blamed this breach on the outdated information technology system provided by the public sector [34]. This could have been avoided if the hospital had adopted a more secure way of managing and accessing healthcare records, in accordance with data laws. This provided the opportunity to suggest a more innovative system that manages data assets efficiently, such as blockchain technology. The hospital focuses on general medical diagnosis, treatment, and tests. We then applied our regulatory readiness assessment framework to a proposed, blockchain-based, healthcare-record-management system for the hospital to improve the confidentiality, integrity, and authenticity of medical records, restrict unauthorized access and give patients full control over their data within the hospital.

The hospital has over 50 staff members, both external and internal, and their patient size has recently increased from 100 patients to 150 patients in the past year. The previous electronic health record system used in the hospital can no longer serve this growing customer database. In the past, there have been losses and comprises of patient information, and fragmented sharing of data. There is also a lack of integrity regarding medical data and patients cannot access their data conveniently.

We propose the implementation of a permissioned blockchain architecture to manage patient data and replace or enhance the current HER system. If set up correctly, patients will have full control over their records, and can revoke access to information. Patients would also be able review doctor's visits, online medical diagnoses, secure data exchange and the interoperability of systems with other health care providers, and secure data collection for ministry and government surveys.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System (accessed on 7 December 2021).
2. Sarmah, S.S. Understanding Blockchain Technology. *Comput. Sci. Eng.* **2018**, *8*, 23–29. [CrossRef]
3. Crosby, M.; Kalyanaraman, V. Blockchain Technology: Beyond Bitc'in. *Appl. Innov. Rev.* **2016**, *2*, 6–19.
4. Lim, M. 81 of Top 100 Companies Use Blockchain Technology. 2021. Available online: https://forkast.news/81-of-top-100-companies-use-blockchain-technology-blockdata/ (accessed on 13 November 2021).

5. Genov, E. The Longest Running Blockchain Has Existed on NYT Pages Since 1995. 2018. Available online: https://toshitimes.com/the-longest-running-blockchain-has-existed-on-nyt-pages-since-1995/ (accessed on 7 December 2021).
6. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2022**, *54*, 1–44. [CrossRef]
7. Charles, W.; Marler, N.; Long, L.; Manion, S. Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research. *Blockchain Distrib. Res.* **2019**, *2*, 18. [CrossRef]
8. Tasca, P.; Widmann, S. The Challenges Faced by Blockchain Technology. *J. Digit. Bank.* **2017**, *2*, 132–147.
9. Dameri, R.P. Improving the Benefits of IT Compliance Using Enterprise Management Information Systems. *Electron. J. Inf. Syst. Eval.* **2009**, *12*, 27–38. Available online: http://search.ebscohost.com/login.aspxdirect=true&db=bth&AN=37568214&lang=fr&site=ehost-live (accessed on 2 October 2021).
10. Haar, R. New Bitcoin ETF Grows at Record Speed. 2021. Available online: https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-etf-approved/ (accessed on 10 October 2021).
11. Dore, K. What the First Bitcoin Futures Exchange-Traded Fund Means for the Cryptocurrency Industry. 2021. Available online: https://www.cnbc.com/2021/10/24/what-first-bitcoin-futures-etf-means-for-cryptocurrency-industry.html (accessed on 13 November 2021).
12. Lin, I.C.; Liao, T.C. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. [CrossRef]
13. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A.; Original, I.; Vieira, T. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 1–13. [CrossRef]
14. Gozman, D.; Liebenau, J.; Aste, T. A case study of using blockchain technology in regulatory technology. *MIS Q. Exec.* **2020**, *19*, 19–37. [CrossRef]
15. Hermstrüwer, Y. *The Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems*; TTLF Working Papers No. 49; Stanford-Vienna Transatlantic Technology Law Forum: Stanford, CA, USA, 2020.
16. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
17. Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
18. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A Survey on Blockchain for Information Systems Management and Security. *Inf. Process. Manag.* **2021**, *58*, 102397. [CrossRef]
19. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops, Kona, HI, USA, 13–17 March 2017; pp. 618–623. [CrossRef]
20. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. B-FERL: Blockchain based framework for securing smart vehicles. *Inf. Process. Manag.* **2021**, *58*, 102426. [CrossRef]
21. Prashanth, J.A.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121–147. [CrossRef]
22. Lapointe, C.; Fishbane, L. The Blockchain Ethical Design Framework. *Innov. Technol. Gov. Glob.* **2019**, *12*, 50–71. [CrossRef]
23. Correia, T.; Correia, H.; Gamito, C.; Kindylidi, I. Evolution of Blockchain Market. 2021. Available online: https://practiceguides.chambers.com/practice-guides/blockchain-2021/portugal (accessed on 12 November 2021).
24. GSMA. Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid. 2017. Available online: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf (accessed on 15 October 2021).
25. Prisco, G. The blockchain for Healthcare: Gem Launches Gem Health Care Network with Philips Blockchain Lab. Available online: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938 (accessed on 27 November 2021).
26. Heston, T. A case study in blockchain healthcare innovation. *Int. J. Curr. Res.* **2017**, *9*, 60587–60588.
27. Batubara, F.R.; Ubacht, J.; Janssen, M. Challenges of blockchain technology adoption for e-government. In Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age—Dgo '18, Delft, The Netherlands, 30 May–1 June 2018; pp. 1–9. Available online: http://dl.acm.org/citation.cfm?doid=3209281.3209317 (accessed on 13 November 2021).
28. Guardtime. Estonia e-Health Authority Partners with Guardtime to Accelerate Transparency and Auditability in Healthcare. 2016. Available online: https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency (accessed on 27 August 2021).
29. Park, J.; Parkm, H. Regulation by Selective Enforcement: The SEC and Initial Coin Offerings. 2020. Available online: https://openscholarship.wustl.edu/law_journal_law_policy/vol61/iss1/11/ (accessed on 13 November 2021).
30. Yeoh, P. Regulatory Issues in Blockchain Technology. *J. Financ. Regul. Compliance* **2017**, *25*, 196–208. [CrossRef]
31. Marques, F.; Albuquerque, M.; Verissimo, D. Blocckchain & Cryptocurrency Laws and Regulation 2022. Available online: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/23Portugal (accessed on 17 November 2021).

32. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A. Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-Like Epidemics: A Survey. *IEEE Access* **2021**, *9*, 95730–95753. [CrossRef]
33. Monteiro, A. First GDPR Fine in Portugal Issued against Hospital for Three Violations. 2019. Available online: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ (accessed on 10 October 2021).
34. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom, Munich, Germany, 14–16 September 2016; pp. 18–20. [CrossRef]
35. Dewey, J. Global Legal Insight—Blockchain & Cryptocurrency Regulations. 2021. Available online: https://www.mlgts.pt/xms/files/site_2018/publicacoes/2020/GLI_Blockchain__Cryptocurrency_Regulation_2021_Portugal.pdf (accessed on 2 October 2021).
36. Lim, M.K.; Li, Y.; Wang, C.; Tseng, M.L. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies, and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
37. Peffers, K.; Tuunaanen, T.; Rothenberger, M.; Chatterjee, S. A design science research methodology for information systems. *J. Manag. Inf. Syst.* **2008**, *24*, 45–77. [CrossRef]
38. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
39. Filippi, P.D.; Hassan, S. Blockchain Technology as a Regulatory Technology. First Monday. *arXiv* **2016**, arXiv:1801.02507.
40. Gupta, S.; Sadoghi, M. Blockchain Transaction Processing. *Encycl. Big Data Technol.* **2019**, *2019*, 366–376. [CrossRef]
41. Kwok, A.; Koh, S. Is blockchain technology a watershed for tourism development. *Curr. Issues Tour.* **2018**, *22*, 2447–2452. [CrossRef]
42. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
43. Kant, N. Blockchain: A strategic resource to attain and sustain competitive advantage. *Int. J. Innov. Sci.* **2021**, *13*, 520–538. [CrossRef]
44. Pal, A.; Tiwari, C.K.; Haldar, N. Blockchain for business management: Applications, challenges, and potentials. *J. High Technol. Manag. Res.* **2021**, *32*, 100414. [CrossRef]
45. Rejeb, A.; Keogh, J.G.; Zailani, S.; Treiblmaier, H.; Rejeb, K. Blockchain Technology in the Food Industry: A Review of Potentials, Challenges and Future Research Directions. *Logistics* **2020**, *4*, 27. [CrossRef]
46. Sung, C.S.; Park, J.Y. Understanding of blockchain-based identity management system adoption in the public sector. *J. Enterp. Inf. Manag.* **2021**, *34*, 1481–1505. [CrossRef]
47. Donovan, A. Blockchain: Developing Regulatory Approaches for the Use of Technology in Legal Services. 2019. Available online: https://www.legalservicesboard.org.uk/wp-content/uploads/2019/10/Blockchain-Developing-Regulatory-Approaches-for-the-Use-of-Technology-in-Legal-Services.pdf (accessed on 3 October 2021).
48. Kshetri, N. Strengthen the Internet of. Securing IT, August. 2017; pp. 68–72. Available online: https://pdfs.semanticscholar.org/e870/9e2906361ade9064cc605b9c7637bec474a0.pdf (accessed on 10 December 2021).
49. European Parliament. Blockchain and the General Data Protection Regulation'. European Parliamentary Research Service. 2019. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed on 5 December 2020).
50. Siegel, S. Is Blockchain HIPAA Complaint? 2018. Available online: https://masur.com/lawtalk/is-blockchain-hipaa-compliant/#:~{}:text=HIPAA%20prohibits%20the%20use%20of,industry%20non%2Dcompliant%20with%20HIPA (accessed on 2 November 2021).
51. Sayegh, E. When Crypto Meets Compliance: Is Blockchain Ready for Enterprise? 2018. Available online: https://www.forbes.com/sites/emilsayegh/2020/07/07/when-crypto-meets-compliance-is-blockchain-ready-for-the-enterprise/#713d7fab4aad (accessed on 11 September 2021).
52. Wang, J.; Wu, P.; Wang, X.; Shou, W. The outlook of blockchain technology for construction engineering management. *Front. Eng. Manag.* **2017**, *4*, 67. [CrossRef]
53. Upadhyay, A.; Mukhuty, S.; Kumar, V.; Kazancoglu, Y. Blockchain technology and the circular economy: Implications for sustainability and social responsibility. *J. Clean. Prod.* **2021**, *293*, 126130. [CrossRef]