data

MDPI

Article

A Blockchain-Based Regulatory Framework for mHealth

Dounia Marbouh [1], Mecit Can Emre Simsekler [1,*], Khaled Salah [2], Raja Jayaraman [1] and Samer Ellahham [3]

[1] Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi 127788, United Arab Emirates
[2] Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi 127788, United Arab Emirates
[3] Heart and Vascular Institute and Quality and Patient Safety Institute, Cleveland Clinic Abu Dhabi, Abu Dhabi 112412, United Arab Emirates
* Correspondence: emre.simsekler@ku.ac.ae; Tel.: +971-(0)2-501-8410; Fax: +971-(0)2-447-2442

Abstract: Mobile health (mHealth) is playing a key role in facilitating health services for patients. Such services may include remote diagnostics and monitoring, chronic conditions management, preventive medicine, and health promotion. While mHealth has gained significant traction during the COVID-19 pandemic, they may pose safety risks to patients. This entails regulations and monitoring of shared data and management of potential safety risks of all mHealth applications continuously and systematically. In this study, we propose a blockchain-based framework for regulating mHealth apps and governing their safe use. We systematically identify the needs, stakeholders, and requirements of the current mHealth practices and regulations that may benefit from blockchain features. Further, we exemplify our framework on a diabetes mHealth app that supports safety risk assessment and incident reporting functions. Blockchain technology can offer a solution to achieve this goal by providing improved security, transparency, accountability, and traceability of data among stakeholders. Blockchain has the potential to alleviate existing mHealth problems related to data centralization, poor data quality, lack of trust, and the absence of robust governance. In the paper, we present a discussion on the security aspects of our proposed blockchain-based framework, including limitations and challenges.

Keywords: mobile health application; mHealth; blockchain; COVID-19; risk management; patient safety; regulation; digital health

Citation: Marbouh, D.; Simsekler, M.C.E.; Salah, K.; Jayaraman, R.; Ellahham, S. A Blockchain-Based Regulatory Framework for mHealth. *Data* **2022**, *7*, 177. https://doi.org/10.3390/data7120177

Academic Editors: Bijan Raahemi and Waeal J. Obidallah

Received: 21 September 2022
Accepted: 8 December 2022
Published: 11 December 2022

1. Introduction

Mobile health, also known as mHealth, have received substantial interest in healthcare practice and research in recent years. mHealth is a term used to define any healthcare practice supported by wireless technology or mobile devices [1]. For example, an mHealth app can assist healthcare providers in monitoring patients' clinical conditions, educating them on self-monitoring, and reinforcing treatment adherence [1–4]. mHealth applications can also support various medical functions, including drug dose calculation [5], clinical reference [6,7], medical records access [8], and clinical decision-making support [9]. Additionally, mHealth apps can help in reducing the frequency of unnecessary hospital visits by patients, therefore decreasing the mobility of patients who are immunosuppressed to high-risk areas [2]. mHealth apps also support workflow management, sharing health records, and storing, enabling more efficient and effective medical practice [10]. During the COVID-19 outbreak, the adoption of mHealth applications turned out to be an essential component to control and manage the pandemic outbreak because of their ubiquity [11,12]. These digital solutions have proved to be readily designed to address prevention, early detection, screening, education, information sharing, and treatment of infected individuals [2].

Even with the great potential for enhancing healthcare, mHealth apps, if inaccurate, misused, or misapprehended, can present the wrong diagnosis and expose users' safety

to risk [10]. Further, these medical apps fall short of providing necessary operational transparency, patient safety management, and incidents and operational failures reporting [13–15]. Vos and Parker [16] stated that if mHealth apps are misused, they have the potential to present a serious hazard. Hence, regulating mHealth apps is both timely and necessary to protect potential risks to users [17]. It should be noted that mHealth apps may fail to allow users/patients to report operational failures or adverse events resulting from the app use. Therefore, a comprehensive regulatory and reporting framework is urgently needed [16]. Creating a regulatory system using a centralized repository would prove cumbersome and requires coordination across all stakeholders and participating parties. It would necessitate expensive, complex, and complicated technical infrastructure to store, access, and provision centralized data for users. As an alternative, blockchain technology offers a potential approach to provide secure, traceable, tamper-resistant, and safe access with improved security.

Blockchain is a shared, distributed ledger and facilitates immutable recording of transactions in a network [18]. This technology has gained attention as an instrument for transferring information between stakeholders based on a distributed ledger that provides complete transparency and immutability of data [19]. A blockchain involves an expanding list of transactions ordered in blocks on a peer-to-peer network. The verified transactions are stored after being digitally signed and timestamped by the sender. This provides a cryptographically undisputable proof of origin and existence of a transaction at any moment in time [20]. This technology is also tolerant against data tampering, manipulation, and network failure [21]. Blockchain technology can reinforce regulatory compliance and oversight since it provides credibility of transactions in a shared and transparent ledger [22]. Blockchain can assist regulators in ensuring compliance with detailed steps required to adhere to complex regulations. The potential benefits of this technology are, therefore, significant and can be summarized in introducing lower costs, improving compliance and governance, decreasing lead times, guaranteeing continuity of processes, and creating an environment that enables secure and easy communication among regulators and those they regulate [23].

The contributions of this paper are presented as follows:

- We discuss the potential benefits of blockchain technology for mHealth apps that enable oversight, pre-certification of app developers, post-market surveillance, and operational failures reporting.
- We present a regulatory framework using blockchain technology to govern the promotion and use of mHealth apps. This framework provides an effective, autonomous, streamlined, and efficient regulatory oversight that ensures the safety and effectiveness of mHealth apps.
- We present an application to highlight the practicality of blockchain for mHealth in managing, assessing, and reporting operational failures and adverse events.
- We present and discuss several open research challenges that prevent mHealth apps from fully exploiting the features of blockchain technology.

The rest of the paper is structured as follows. Section 2 introduces the mHealth applications and potential benefits of blockchain technology in healthcare. Section 3 briefly introduces the study design, while Section 4 outlines the proposed regulatory framework for mHealth. Section 5 presents a case study for a possible application of the framework in Diabetes mHealth applications, while Section 6 discusses compliance, governance, and open challenges. Finally, Section 7 presents the conclusions, limitations of the study, and opportunities for future research.

2. Related Work

This section provides the necessary background for developing a trusted regulatory framework for mHealth apps using blockchain technology.

2.1. mHealth Applications

mHealth apps have become popular among mobile users [24]. These apps are software programs on mobile devices, including smartphones and tablets [25]. mHealth apps proved to be very valuable, not only to their direct users, but also to medical professionals who benefit from their usability for monitoring patients' progress [26]. Medical apps are used in diagnosis and treatment, electronic prescribing, coding and billing, patient monitoring, and e-learning [27]. These apps can greatly empower providers and enhance clinical decision-making and analysis [24].

While medical apps offer many benefits, they may also pose several risks, especially those used in clinical diagnosis [13,15]. Recent investigations have provided evidence that third-party developers do not cite or offer references for the material provided in the app [28,29]. In a study that investigated the source of information supplied in cancer-related apps (i.e., chemotherapy dose and regimen calculators, cancer staging apps, and radiological imaging apps), the authors discovered that only 55.8% of the apps provided scientifically validated data [30]. In another study, the authors looked at the reliability of opioid conversion apps. They found that just half of them were reliable, while the other half did not reference their dose conversion guides [31]. These studies indicate that mHealth apps can be helpful as a medical reference, however, their content quality might jeopardize patient care.

In addition to the apps' information quality, another concern is the potential safety risks to users. The app developers are expected to demonstrate clinical validation and consultation with healthcare providers and trained staff to deliver accurate and safe information. Despite this, earlier studies showed limited collaboration between app developers and healthcare providers during the app development process [14].

Furthermore, some mHealth apps do not go through a formal evaluation before being launched to the public [14]. While there are various app stores available (e.g., Apple Store and Google Play [32]), mHealth developers might be only required to submit app details for evaluation by such stores While an assessment is executed to guarantee that the apps have no major technical issues and function as intended, the quality of the apps' medical content may not be comprehensively reviewed [17,33]. As a result, several apps of poor quality can slip through the assessment procedure. In addition to the alarming lack of a robust app assessment process, there is also the general absence of regulatory oversight. In fact, due to the complexity and diversity of the software products, their regulatory oversight has proven to be challenging [14].

The FDA did not explicitly address the regulation of mHealth apps until 2011, with the issuance of draft guidance on the subject [34]. The FDA, for example, does not regulate apps that give contextually relevant access to clinical material used in medical practice (for example, apps that check for drug–drug or drug–allergy interactions) [3]. Likewise, the FDA does not evaluate apps that offer clinical practice guidelines to providers or other treatment recommendations for a specific medical condition [35]. Since many of these apps are used to support critical treatment decisions (for instance, determining drug choice or drug dose), it is imperative to hold app developers responsible for the accuracy and quality of the content provided [14]. Additionally, given the sheer volume of mHealth apps and their quick adoption by users, it is imperative to review apps' current regulatory oversight process to verify if the existing frameworks fit their intended purpose [33].

2.2. Blockchain Technology

Blockchain technology is a shared and distributed ledger used for tracking and storing transaction records. This technology offers a shared and permanent record of peer-to-peer transactions constructed from connected blocks of transactions and kept in a digital ledger [36]. Blockchain relies on proven cryptographic techniques without pre-existing trust between the stakeholders [37]. There is no central authority in a blockchain that controls the network; transaction records are stored and distributed among all system members. All participants are aware of interactions with the blockchain and require network verification

before the information is added, allowing trust-less communication between network participants while recording an immutable audit trail of all interactions [38]. Blockchain technology can facilitate data fraud detection and operational efficiencies in addition to enforcing regulatory compliance and governance. These blockchain features offer unique benefits that traditional centralized systems cannot achieve [39].

One of most imperative concepts linked with blockchain technology is smart contracts [40]. As a computer program or a transaction protocol, smart contracts provide substantial benefits in traceability and immutability after their deployment [41]. Most blockchain applications are programmed using smart contracts [42]; therefore, their successful development is vital in successful blockchain implementation. Decentralization is another crucial aspect of blockchain technology since it removes intermediaries from the network, lowering transaction fees and improving data security. Furthermore, blockchain technology has intrinsic characteristics, such as cryptographic methods and time-stamped records, traceability, data integrity, immutability, and transparency [43].

Blockchain technology is well suited to tackling some of the particular issues associated with regulating mHealth apps. Blockchain architectures enable near-real-time decentralized information exchange across stakeholders when trust is limited (i.e., between the regulated and the regulator). Further, they give means for trusting the validity of compliance data and provide an immutable audit trail for transactions [44]. Hence, blockchains can make transaction reporting easier without jeopardizing regulated parties and regulators' general roles and obligations, improving risk transparency [22].

3. Study Design

In order to understand the potential implications of the blockchain technology in mHealth, the following steps are taken in this study design to lead to a blockchain-based regulatory framework. First, data and information on mHealth regulation is methodically collected to help identify requirements of the proposed framework. At this stage, the literature review and examples from the healthcare industry are primarily used to help understand the current mHealth regulation practice. This stage also helps identify the key stakeholders, challenges, and potential blockchain features that can be beneficial in providing safer regulatory framework for mHealth apps.

Further, a case study on diabetes mHealth application is demonstrated to present two important safety functions, namely risk assessment and incident reporting, where blockchain may have unique contributions in an mHealth context. Lastly, we discuss compliance, governance, and various open challenges regarding the use of blockchain in mHealth environment.

4. Blockchain-Based mHealth Applications

This section describes our system and its stakeholders and presents our proposed solution.

4.1. Blockchain for the Regulation of mHealth Applications

Blockchain technology can provide substantial benefits to the regulation of mHealth apps. For instance, data integrity, security, reliability, accessibility, and immutability of all transactions are fundamental characteristics that can improve mHealth [45]. Additionally, the ability to add verifiability and authentication of stakeholders' identity, primarily mHealth providers, are characteristics that can increase the trust in and safety of these services. Blockchain also can alleviate several issues such as the centralization of data, poor data quality and documentation, lack of trust, and the absence of better governance. With blockchain, regulators would not have to gather, store, reconcile, or aggregate data because blockchain data is decentralized by design. All transactions are immutably recorded on the distributed ledger, resulting in a complete, secure, irrevocable, and permanent record [39].

With the decentralized nature of blockchain, regulators and other stakeholders would maintain the same copy of the ledger, saving the entire chain a significant amount of money. Further, having a secure regulatory framework provides safety assurances. It

would also create credibility and trust among users and app providers and can be designed to comply with other international standards, facilitating market entry. Table 1 summarizes the challenges that the current mHealth system faces. Further, it presents opportunities through blockchain features to benefit in a regulation oversight framework. Moreover, it presents the stakeholders that will play a role in the process and potentially benefit from these opportunities.

Table 1. Requirements and potential benefits of blockchain in the regulation and post-market surveillance of mHealth applications.

Current Problems	Challenge Description	Blockchain Features	Remarks	Stakeholders
Data Quality and Documentation				
Centralized system [46]	Centralized data storage and processing platforms often result in data inconsistency [46], increase the cost of completing transactions, and encourage data beautification and falsification. They are hard to maintain and expensive [47].	■ Decentralization: discard any third-party or central authority [19] ■ Trust: the trust moves from a central party to an open-source code [48] ■ Cost-saving: elimination of third parties [49]	Decentralization eliminates the concentration of power of the controlling party, which is an essential condition to reach efficacy, transparency, and trust. It also eliminates the high communication costs thanks to the distributed architecture [19].	■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA) ■ Researchers/Academics
Lack of transparency [50]	Most apps do not contain information about content/app creator or their background. It is vital to prove that the developer has the medical expertise and knowledge to provide high-level information quality [33,51].	■ Using dashboards, developers can see how they are performing among relevant metrics ■ Decentralized: it makes safety issues transparent to stakeholders ■ Immutability of records [52]	Blockchain uses a distributed ledger; therefore, the data details are recorded identically in various locations, providing complete transparency [48,53].	■ Patients ■ Providers ■ Insurance providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)
Lack of app content quality check [28,54]	Some developers fail to cite or provide references to the app's content. It is also hard to keep track of the steps required by regulation to ensure excellent quality [28,29].	■ Smart contract: they allow pre-specification of the quality steps before triggering the transaction [42,48] ■ Enhanced data quality check [55,56]	Blockchain can help regulators in keeping track of the quality steps required by complex regulations [55].	■ Patients ■ Insurance providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)

Table 1. *Cont.*

Current Problems	Challenge Description	Blockchain Features	Remarks	Stakeholders
Low data security [54]	The current regulatory framework operates on a centralized database which poses many data security risks, including a single point of failure [28].	■ Encryption: once a transaction gets approved, it is then encrypted and connected to the previous one [45] ■ Consensus: before recording transactions, participating parties must agree to it [48] ■ Distribution: data are stored across a network of computers, which makes it hard to compromise [44]	By creating an immutable and encrypted system end-to-end, preventing fraudulent and unauthorized activities becomes an easy task. It would also prevent the duplication of the app software in abundant duplicates and can spread outside the developer's control [57].	■ App Developer ■ Patients ■ Agency Reviewer (i.e., FDA, MHRA)
Governance and Accountability				
No pre-certification of app developers [17]	The app developers (individuals and companies) do not undergo a pre-assessment to check if they meet excellence standards and demonstrate a previous history in developing safe and effective apps [17,33].	■ Streamlined oversight [22] ■ Streamlined communication [58] ■ Register approved developers [57]	Blockchain would lend its distinct decentralization advantages of DLT to enable streamlined oversight and communication [58].	■ Patients ■ Providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)
The inconsistent app appraisal process [33]	Currently, app developers struggle with the uneven distribution of information, resulting in an inconsistent appraisal process [17]. As a result, developers do not know what to expect when appraised and do not fully understand the criteria.	■ Consensus algorithm: apply consistent rules and obligations to developers [48] ■ Validation and verification before trigging a transaction ■ Unified network protocols and standards [48]	Blockchain would play the role of proof-of-process so that all the required steps are easily traceable and verifiable. Blockchain can also maintain rules and standards to allow developers to understand the appraisal process [39,48].	■ Patients ■ Providers ■ Insurance providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)

Table 1. *Cont.*

Current Problems	Challenge Description	Blockchain Features	Remarks	Stakeholders
Lack of control over app upgrades [59]	Developers have fast development cycles and provide regular updates to their software. Further, the app software may be in abundant duplicates and can spread outside the developer's control. It is essential to track and trace the software configuration and software changes [59].	■ Tamper resistance and evidence of tampering attempts ■ Immutability of the ledger: an immutable audit trail of modifications and upgrades [60] ■ Fraudulent activity can be quickly detected [61]	Thanks to the immutability of blockchain, any app alterations, changes in intended use, or developments of functionality will be recorded in the ledger. This would allow software iterations and changes to occur under appropriate controls [60].	■ Patients ■ Providers ■ Agency Reviewer (i.e., FDA, MHRA)
Lack of post-market surveillance [62]	At present, there is an absence of post-market monitoring of developed apps. Developers do not have access to information about how this app performs in the market to support advanced functions. Regulating bodies also do not get access to verify if the product meets its promised effectiveness of safety [62].	■ Streamline post-market surveillance and review [62] ■ Access to complete app performance data ■ Access to users' incident reports ■ Identify fraudulent and unqualified app developers [62] ■ Verification of continued safety and effectiveness	Thanks to blockchain, it will be easier to verify compliance with safety requirements and assure that the app complies with its intended use needs and operational requirements [39]. The regulatory authority (i.e., the FDA) can interpret this real-world information to evolve the product's safety and address any evolving risks using collected and aggregated data.	■ Patients ■ Providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA) ■ Researchers/Academics
Adverse Events Reporting and End-user Safety				
Inability to report issues with apps [63]	Currently, it is not possible to report the issues arising from medical apps. As a result, it is hard to ensure safe, effective, and secure apps since no practices are integrating appropriate review activities [63].	■ Credibility: a single source of trusted data in a distributed ledger [64] ■ Near-real-time communication [58] ■ Secure communication across stakeholders [57]. Mainly regulators and end-users	Blockchain can mitigate this issue by offering a ledger that is immutable and accessible to all stakeholders [60]. It also reduces the complexity and allows end-users to report adverse events or operational failures more quickly.	■ Patients ■ Providers ■ Insurance providers ■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)

Table 1. *Cont.*

Current Problems	Challenge Description	Blockchain Features	Remarks	Stakeholders
Adverse Events Reporting and End-user Safety				
Low safety [29]	Due to the absence of solid regulations, medical apps are not being monitored or managed for risks along multiple dimensions such as user-based, application-based, user environment-based, and security-based. This results in compromised safety for the users [29].	■ Access to viewable and trusted data about the app and developer ■ Verification and validation of data before trigging a transaction ■ Identification of fraudulent activities [61] ■ Prevention of compliance violation	With blockchain, safety control and audit can be enhanced due to the streamlined process and audit trail capability [51]. End-users can be confident about the veracity of the information, the app's effectiveness, its safety, and developers' skills.	■ Patients ■ Insurance providers
Unrestricted market entry [63]	At present, any app developer, even without medical knowledge, can create a medical app [28,63]. These apps are often not safe, non-legally compliant, and do not operate according to community expectations.	■ Limit the network for pre-certified and authorized developers ■ Verify the skills of developers ■ Prevention of compliance violation	This blockchain-based solution would limit unqualified app developers from entering the market and stimulate innovation among developers to create inventive and highly compliant apps.	■ App Developer ■ Agency Reviewer (i.e., FDA, MHRA)

mHealth apps collect data through interactive questionnaires, separate accessories linked to the mobile device, or features in the mobile device such as the camera, microphone, or motion sensor [34]. Apps may leverage medical algorithms or calculators to process these data and generate personalized diagnosis and therapy recommendations. mHealth apps can make the collection of granular patient data easy and possible [65]. These data are susceptible, and storing them in centralized databases may risk leakage or exposure. However, with the help of blockchain, we can enhance the efficacy of mobile-based healthcare applications for sharing and collaborating data [62]. Using a user-centric system of data sharing, we can design a system that connects patients, healthcare providers, insurance providers, and, lastly, the blockchain network. In mHealth, this technology can also be very beneficial in the following ways:

Improve remote prescription adherence. Smart contract-powered mHealth apps can assist in automating prescriptions and refill notifications. This technology can also guarantee compliance to medication while minimizing hospital re-admissions and poor medical performance. It can also help care providers facilitate the process to build morale and patient involvement.

Improve contact with providers. mHealth technology based on the blockchain can increase the ability to unify the health system. It can also enable healthcare providers, patients, and hospital staff to connect using encrypted texting and messaging, video calls, and access to mobile health records. Besides, it can guarantee seamless system interoperability, therefore lowering the expenses and delays related to fragmented collaboration.

Activate remote monitoring of patients. Healthcare providers can remotely control patients' medical conditions with blockchain-based mHealth apps. Patient remote monitoring can be achieved by analyzing the immutable data collected by IoT-enabled wearable devices, such as wristbands, fitness trackers, and watches. Hence, patients can be confident that their condition is being controlled while there are no privacy breaches or data misuse due to blockchain-powered attributes.

Improve diagnostic quality. By giving healthcare providers access to patient medical data with minimal errors, blockchain mHealth apps would reduce their burden. Physicians can also diagnose patients effectively with access to their records and handle more patients daily. Moreover, patients will determine which data they want to share with which diagnostic provider.

Figure 1 illustrates an example of a potential use case of blockchain in mHealth, a blockchain-based data-sharing framework for mHealth. This proposed framework illustrates how data are collected from mobile devices and aggregated in the blockchain network. The figure illustrates the case of a diabetic patient who uses a diabetes wearable device and requires remote monitoring. As illustrated, the data collected from the wearable device are uploaded into the decentralized storage system. These data are then analyzed by the healthcare provider to monitor and control the patient's condition remotely.

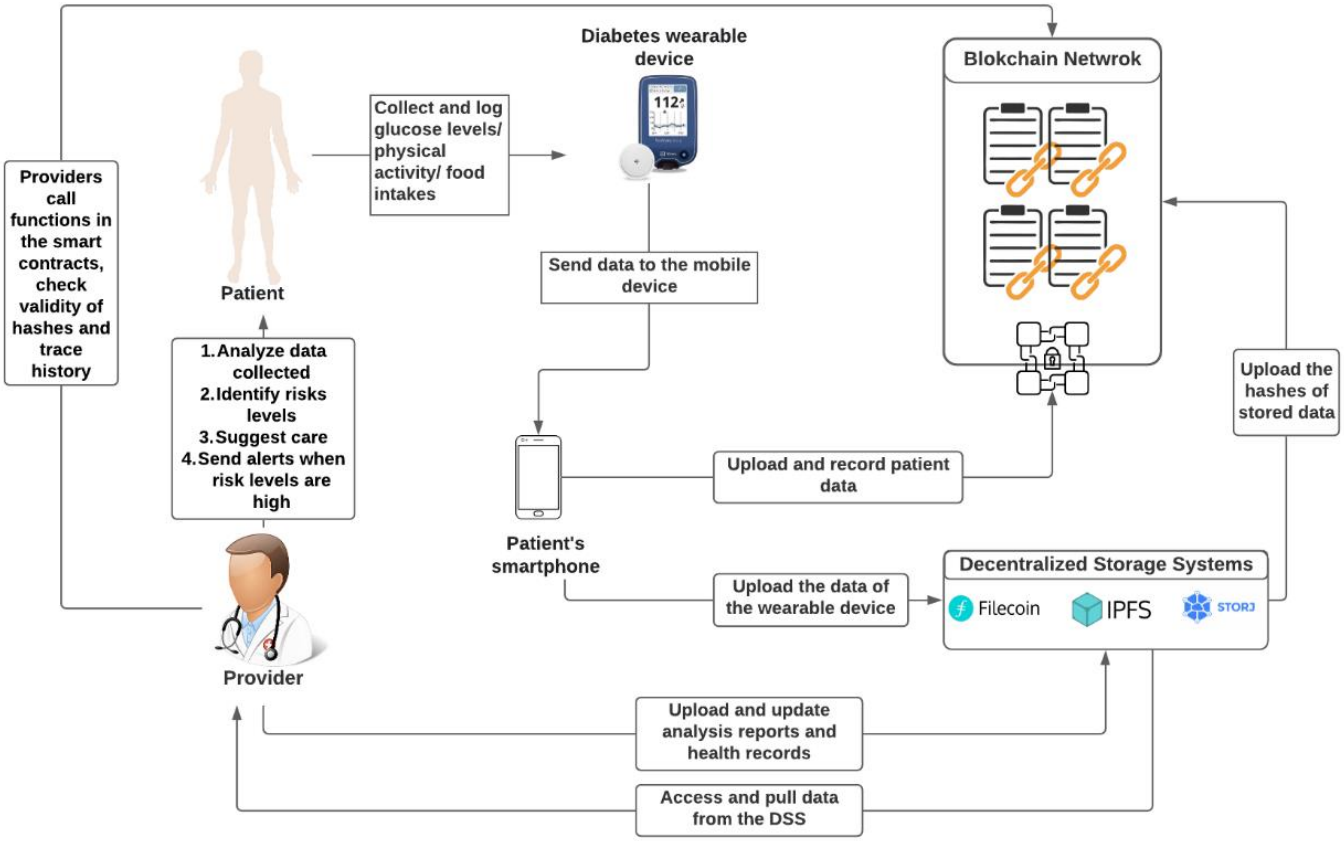

Figure 1. Blockchain-based data sharing Framework for mHealth app.

4.2. System Stakeholders

Creating a blockchain-enabled system for regulating and monitoring mHealth apps involves several stakeholders. It is important to note that the successful information exchange among stakeholders is vital in designing an information technology system [66,67]. Potential stakeholders are patients, healthcare providers, apps developers, regulatory entities, and researchers. Table 2, below, summarizes their key roles and responsibilities.

Table 2. Roles and responsibilities of stakeholders in mHealth.

Entity	Role	Responsibilities
Patient/User	Use the mHealth app and report any issues that might arise.	- Grant access to desired parties - Deny and revoke data access from any other parties
Healthcare Providers	Access the mHealth app and report any issues that might arise.	- Report and update health data - Warn authorities about the device compliance
Researchers and Academics	Develop mHealth apps and devices and explore improvements and potential contributions.	- Research new methods to improve processes - Use the data to obtain more insight and identify trends in healthcare

Table 2. *Cont.*

Entity	Role	Responsibilities
App Developers	Build mHealth apps with the intent of helping users manage their medical conditions while assuring compliance with the applicable regulations.	- Lower the complexity of the app and provide good functionality - Follow safety regulations when building an app - Update the app in case of failures - Perform a post-market surveillance - Monitor and act upon any adverse events or complaints
Regulatory Authorities (accredited parties)	Review and generate an action plan to develop guidance. Pre-certify adherent app developers who proved to have a robust safety culture.	- Develop guidance and action plans - Certify app developers that adhere to safety guidelines and rules - Analyze and monitor aggregated data
App Store Platform (i.e., Google Play, App Store)	Review the app code and provide access to app content on the platform.	- Attest and certify the app code

4.3. System Overview

As illustrated in Figure 2, our proposed system will support the development of a regulatory model that can offer an efficient and streamlined oversight of medical apps. This framework assures limiting the market to developers who have a robust safety culture, continuous improvement, quality, and who are devoted to monitoring their products once launched to the public.

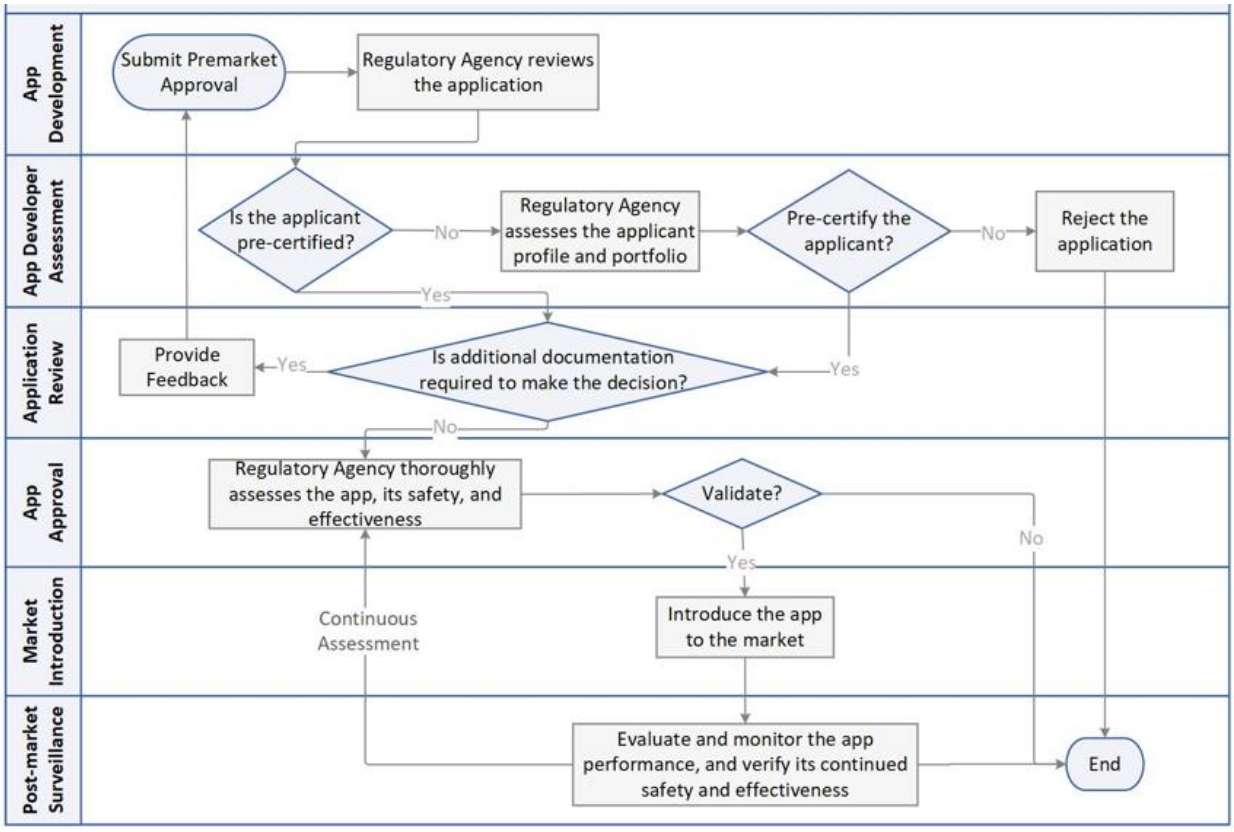

Figure 2. Flowchart of the blockchain-based framework.

This proposed solution intends to investigate and inspect the app developer first, rather than the product. As a result, this regulatory framework will ensure responsiveness, safety, and effectiveness when problems arise to help ensure app users continue to have access to safe and effective apps. We should also note that the justification for the use of blockchain features (e.g., consensus algorithm, smart contracts, and distributed architecture, etc.) that mHealth regulatory framework can benefit is comprehensively addressed in Table 1.

Figure 3 illustrates the system overview of our proposed regulatory framework that includes various smart contracts, as follows:

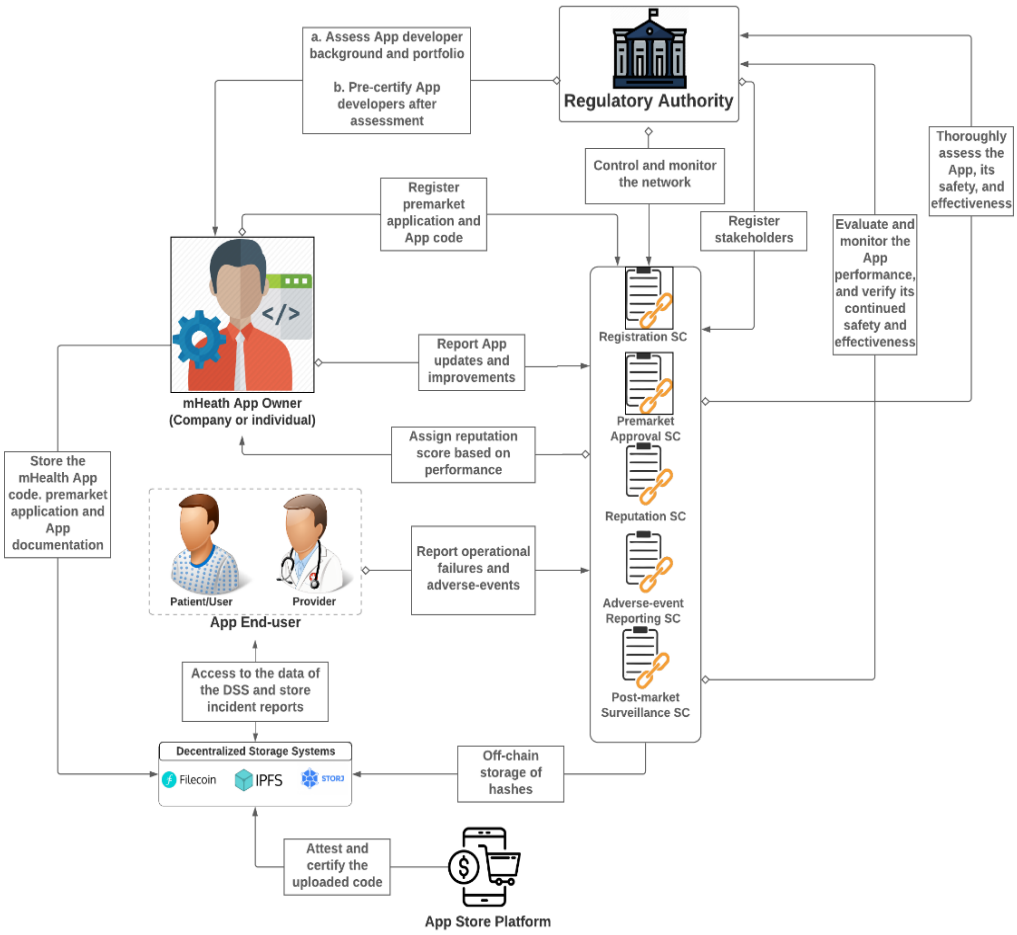

Figure 3. Overview of the blockchain-based regulatory framework.

Registration Smart Contract. This smart contract is responsible for registering app developers (companies or individuals), app code, and other relevant stakeholders.

Pre-market Approval Smart Contract. This smart contract is concerned with the appraisal process to evaluate the safety and effectiveness of apps.

Reputation Smart Contract. This smart contract involves assigning a reputation score to developers derived from assessing their performance and trustworthiness. Therefore, the reputation is positively affected by reputable and qualified developers and negatively affected by fraud.

Post-market Surveillance Smart Contract. This smart contract is responsible for verifying the continuity of safety, effectiveness, and performance of medical apps once in the market.

The present solution also integrates off-chain storage systems, such as cloud storage, or a decentralized storage system, such as Filecoin, Interplanetary File System (IPFS), or StorJ. Off-chain storage is used for storing, accessing, and keeping track of large-size digital content such as pre-market applications, app code, and documentation.

5. Case Study: Diabetes mHealth Applications

Diabetes (diabetes mellitus) is a chronic condition involving several stakeholders besides the patient, for example, the healthcare provider, endocrinologist, and multi-specialty team, including eye specialists, nephrologists, and cardiologists [68]. As a result, patients with diabetes frequently create vast amounts of data, including physical activity, self-measurement of blood glucose, continuous glucose monitoring (CGM), and blood pressure [69]. Therefore, mHealth apps can effectively provide a platform to track health condition and health-related data [70].

People with chronic illnesses, particularly diabetes (type 1 and 2), have found mobile health technologies quite beneficial. Patients who have diabetes must keep track of much information about their condition, including blood sugar levels, meals, exercise, and prescriptions, all of which mHealth apps can support [69,71]. The mHealth apps can be generally categorized into three classes: apps that serve as stand-alone clinical devices, apps used for wellness tracking, and apps that exhibit, download, or make use of data from medical devices that diagnose, monitor, prevent, or treat an illness (i.e., CGM, insulin pump) [72]. Apps that are designed to assist in diabetes management are the most commonly used among nearly half a million apps in the market [73]. Given that more than 2.7 billion people have access to smartphones and over half a billion people use mHealth applications for physical exercise, diet, and chronic disease management, diabetes apps have the most considerable potential for impact [72,74].

5.1. Risk Assessment

mHealth apps such as those used for diabetes might pose a significant risk to users and affect confidence among healthcare providers and patients if poorly designed. For example, apps used for diabetes diagnosis and therapy, such as the calculators used for drug dosage recommendations, may directly affect the user's safety [29]. A recent study investigated the accuracy and clinical suitability of apps calculating insulin dose and identified that only 1 out of 46 apps was issue-free [75]. The poor quality of apps, their incompleteness regarding information and functions, and poor ease of use were the most frequently mentioned disadvantages of use [5]. Hence, risk categorization of the medical apps is vital to define their level of security, quality, and corresponding regulation model. The FDA leverages the risk category framework established by the International Medical Device Regulators Forum (IMDRF) to advise the risk category of medical apps. For example, an app that provides essential information about the treatment/diagnosis of a critical health situation is regulated and controlled as a Class IV device. Table 3 explains how to define the risk category of apps based on the condition or status of the user and the significance of the information it provides.

Table 3. Risk classification of mHealth apps.

Health Situation or Condition of User	Information Significance Provided by the App to Healthcare Decision-Making		
	Treat or Diagnose	**Drive Clinical Management**	**Inform Clinical Management**
Critical	**IV**	**III**	**II**
Serious	**III**	**II**	**I**
Non-serious	**II**	**I**	**I**

Apps in Class I will necessitate only an inspection to be conducted locally, those in Class II will need an additional formal risk assessment, and those in Class III and IV will need to comply with formal regulations and criteria set by regulating authorities such as the FDA, due to their high potential of resulting in harm [13]. Table 4 further explains the differences between the four classes.

Table 4. Risk Assessment of mHealth apps.

	Criteria for Determining App Category	Example of App Functionality	Regulation Model
Class I: Low impact	App offers information about: ■ The management of an illness in a non-serious situation ■ Informing the medical management for a condition in a non-serious state	Patient e-learning and education, EHR access, BMI calculators, access guidelines, other learning material [13].	Provider self-assessment or an accredited third party
Class II: Medium impact	App offers information about: ■ Treating or diagnosing a condition in a nonserious state ■ Driving medical management of a condition in a severe state ■ Informing medical management of a condition in a critical state	Inter-professional consultation and referral, drug conversion, entering treatment requests [13].	Formal assessment and regulation by government body: e.g., FDA
Class III: High impact	App offers information about: ■ Treating or diagnosing a condition in a severe state ■ Driving medical monitoring and management of a condition in a critical state	Diagnostic support apps, specialist apps, patient decision app, medical calculators [13].	Formal assessment and regulation by government body: e.g., FDA
Class IV: Very high impact	App gives information for treating or diagnosing a condition in a critical situation	Closed-loop apps and clinical decision support tools, control devices [13].	Formal evaluation and regulation by regulatory authority: e.g., FDA

It might be impossible to detect all app-related issues [29] because some problems become apparent only after thorough testing. Therefore, it is critical to comprehend and quantify the risks that medical apps pose to inform safe clinical use of mHealth apps and potential regulation and guidance [29]. The first step in this process is to determine that harm the mHealth app can cause and allow for its easy reporting.

5.2. Incident Reporting

One key area of the current medical diabetes apps is insulin calculation [68]. The insulin calculator helps calculate the right amount of insulin or carbs for correction or meals. Patients may find it difficult to spot errors when using a calculator. Patients with low numeracy may be unable to "sense check" odd outcomes due to a lack of intuitive basis [29]. Users may also pay less attention to calculating and evaluating the app's outcome during social events where a calculator should be used, such as mealtimes. App disclaimers frequently invited patients to examine the calculated dose in-app disclaimers. However, more than two-thirds of them failed to disclose details about the underlying formula that would allow this, and only a small number of apps flagged odd input or output [13].

Our literature review shows that app users are faced with many critical issues, such as poor information quality, gaps in features, and improper response to their needs [28,29,54]. mHealth apps with therapeutic and diagnostic attributes, such as calculators that recom-

mend a dose of medication, can easily affect health outcomes [75]. Hence, structured incident reporting is crucial as it allows the identification of deficiencies that make calculators inaccurate and unsafe [75]. This suggests that users' involvement in incident reporting will facilitate problems identification and resolution. Reporting issues with the app will also allow users to provide significant insights about app functionality and reliability, support determining if the app is appropriate for users to perform required tasks, and might lower the costs of fixing problems that may be identified later. Users can also give their feedback to app developers and regulatory authorities such as the FDA [29].

Figure 4 illustrates the risk management of an app that recommends an insulin dosage. As can be seen, in the event of a failure (e.g., calculator gives an erroneous dose recommendation that may result harm the users), the users can report the incident to providers and log the incident to the network. The regulatory body then reviews the incident and the developer's certification and takes suitable action accordingly.

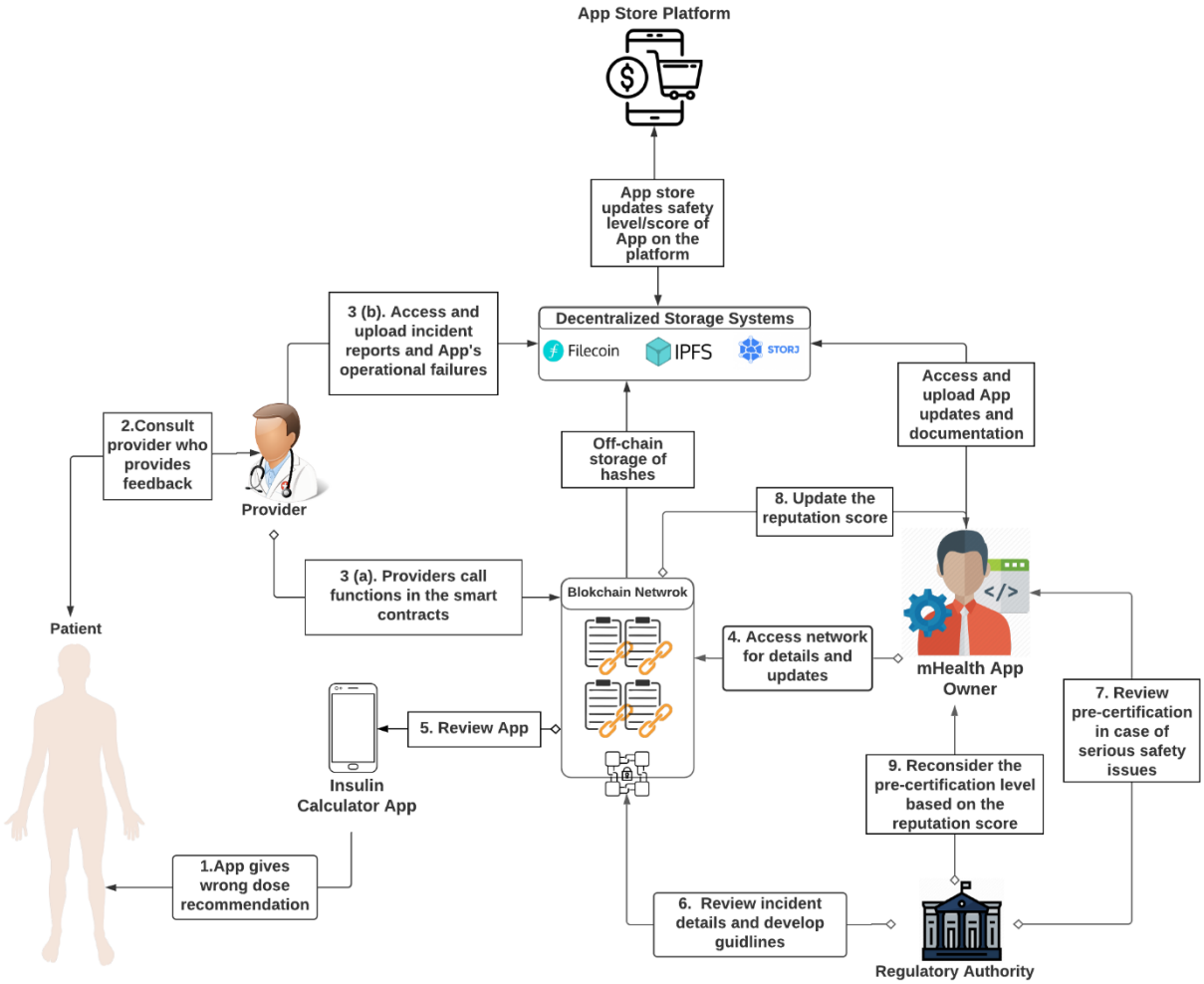

Figure 4. Blockchain-based risk management framework for mHealth apps.

6. Discussion

The application of mobile technologies in healthcare is promising as it enables convenient and quick data access. It offers various benefits, including tailored recommendations and the ability for individuals to receive health services at any time and from any location. For instance, blockchain technology can easily enable the building of an mHealth infrastructure that allows remote patient monitoring (RPM) [76]. This technology can also enable tailored health management and monitoring and contributes to a health system that is more decentralized [25]. However, the widespread use of medical data has long been

a complex and sensitive topic, with privacy and security being significant concerns. This section overviews the main challenges in leveraging blockchain for mHealth. Moreover, it presents the existing methods to address them.

6.1. Compliance and Governance Assessment

Due to the blockchain's decentralized nature, regulatory agencies in certain parts of the world have imposed data protection regulations to secure medical records from various threats and attacks. The most prevalent data protection regulations are the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) [77]. Blockchain implementations must, therefore, comply with the existing regulatory standards to ensure their usability and practicality within the healthcare industry. In blockchain-enabled solutions, the role of HIPAA and GDPR becomes more relevant and complex as it becomes hard to define the legal boundaries and ecosystem for blockchain technology [78].

Although blockchain offers several opportunities in achieving better interoperability and health data sharing, this technology can break some regulatory frameworks (i.e., GDPR and HIPAA). The HIPAA and GDPR are responsible for regulating the collection, processing, and securing of personal data, including protected health information (PHI). Therefore, streamlining blockchain's applicable agreements and interoperability is essential to preserve its legal framework. For instance, blockchain can break jurisdictional boundaries, since nodes can be found anywhere in the world on a ledger [79]. In addition, because of the immutable nature of blockchain, data stored on-chain cannot be deleted, violating patients' privacy. Blockchain can also oppose the data minimization principle of GDPR, which states collecting only the essential data to achieve a specific purpose [80]. Our proposed solution in this study partially mitigates these limitations by storing the medical records on a decentralized storage system, and hence the records can be deleted.

Furthermore, it is essential to identify the different blockchain actors' roles with respect to the processing. Defining who can act as the controller is crucial since people whose personal data are stored on the ledger must be informed about which party they can contact to exercise their rights effectively. In our proposed solution, the data controller is the health regulatory authority (e.g., FDA). The controller is also responsible for adding new actors, removing others, and assigning reputation scores to the mHealth app developers based on their performance. In addition, controllers/processors should consider their responsibilities to assign a data protection officer, implement data protection, and oversee data protection impact assessments [80].

6.2. Open Challenges

Scalability. Currently, blockchain technology faces a limitation that, sometimes, hinders its adoption. This limitation is the inability to process several transactions at a reasonable rate. While this technology lowers the risk of fraudulent and malicious conduct, it also lengthens the time it takes for transactions to settle. For instance, the bitcoin blockchain can only handle seven transactions per second (tps), compared to other transaction processing systems that can handle tens of thousands [81]. Visa Inc., for example, can process 4000 tps, while the Universal Trade Capture (UTC) can process 47,000 tps [82]. Sharding techniques, lightning the network, and proof-of-stake (POS) are some of the several solutions that can be implemented to solve this issue [83].

Storage. The regulation processes such as developer pre-certification, app appraisal, post-market surveillance, and incident reporting produce a large amount of data [13,53]. These generated data can be in several shapes, including files or images, that assure that the designed apps are compliant with safety principles. In the case of our proposed solution, each node would be storing a copy of data which might result in a shortage of the blockchain's storage capacity [84]. The decentralized storage solutions such as IPFS and Filecoin can be a great way to overcome storage limitations in blockchain [85]. For instance, a decentralized storage system such as the IPFS can generate permanent hashes

of the stored data. These hashes are immutably stored on the blockchain network to ensure that stored data are not altered [81].

Privacy and Identity. Ensuring requirements such as the privacy of users and data and anonymity by the underlying blockchain-based solution is crucial to the participants regulating medical apps. All participating parties may see transactions on a public blockchain. However, the public address of each participating party can be used to identify it. Although the public address is pseudonymous, suspicious actors with some prior information can manipulate the links between the transaction user's real-world identity and public addresses [81]. In particular, the public blockchain platforms are more susceptible to enduring several attacks since the pseudonymous addresses, transactions, and other user data are publicly available. On the other hand, private blockchains such as Hyperledger Fabric and Besu run in a more controlled environment, making them more secure than public blockchain platforms [86].

Expenditures on Infrastructure. The adoption of emerging technologies, such as IoT and blockchain, may help lower operational costs, improve productivity, and achieve advanced operational efficiency. However, because of the level of innovation required by these solutions, health organizations need to devote a substantial amount of capital to implementing, managing, and maintaining these technologies. As a result, these practices and availability of various platforms [87–89] would necessitate balancing the cost–benefit analysis. Furthermore, the blockchain's perceived risks associated with being immature, its high fees of initial employment, and the likelihood of disrupting existing practices may pose other substantial issues to the day-to-day processes and businesses [90].

7. Conclusions

In this study, we have reviewed the state of the art on mHealth apps and blockchain technology. We presented the potential benefits of integrating blockchain technology with mHealth monitoring and governance. Further, we discussed the regulatory oversight framework for apps' governance and an incident reporting system to manage risks through a use case.

The number of mHealth apps is constantly increasing, as they prove to be beneficial, quick, and easy access to information. They aid in monitoring chronic patients, improving medication administration, and networking people in similar conditions. The recent evolution of mHealth services and applications has resulted in significant advances and innovative mobile technologies into conventional health systems, shifting the focus from healthcare providers to patients. To achieve further advances in mHealth, regulating the current system and enforcing strict oversight on apps developers is paramount, due to concerns about patient safety and well-being.

The mHealth apps market is challenging to regulate since it is a fast-paced market with several new market entrants every year. However, blockchain technology can be a great solution to address this challenge. A blockchain-based regulatory framework may result in transparent and effective processes addressing potential safety, quality, and privacy concerns. Further, such regulations would recognize and leverage the exclusive aspects of mHealth application use in the future. As mHealth apps become ubiquitous, regulatory monitoring also becomes more imperative. As an emerging technology, blockchain technology can also help protect public health and maintain user confidence in mHealth apps and services. However, more research is needed to conduct a feasibility analysis considering tradeoffs between cost and security.

Our study has limitations that can be addressed in future studies. First, it should be noted that this paper provides a conceptual framework for blockchain-based mHealth regulation with no empirical evidence. Although we conceptually introduced smart contract and additional technologies (e.g., IPFS for mHealth data storage) in the framework, we did not evaluate their implementation with relevant security and cost analysis. Therefore, future studies can benefit from exploring the feasibility of smart contracts, as they play a pivotal role in blockchain technology [40,41]. Such studies may provide substantial and

comprehensive guidance on potential success criteria and barriers for the blockchain-based mHealth implementations.

Author Contributions: Conceptualization, D.M., M.C.E.S. and K.S.; Methodology, M.C.E.S.; Validation, M.C.E.S., K.S., R.J. and S.E.; Formal analysis, M.C.E.S.; Resources, M.C.E.S.; Writing—original draft, D.M. and M.C.E.S.; Writing—review & editing, M.C.E.S., K.S., R.J. and S.E.; Visualization, D.M., M.C.E.S. and K.S.; Supervision, M.C.E.S., K.S. and R.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Khalifa University of Science and Technology under Award CIRA-2019-001 and RCII-2019-002-Research Center for Digital Supply Chain and Operations Management. The funding body had no direct involvement in the de-sign, data collection, analysis, and interpretation, or in writing the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declared no potential conflict of interest with respect to the authorship and/or publication of this article.

Abbreviations

GDPR: General Data Protection Regulation; HIPAA: Health Insurance Portability and Accountability Act; FDA: Food and Drug Administration; IMDRF: International Medical Device Regulators Forum; PGHD: Patient-Generated Health Data; IPFS: InterPlanetary File System; RPM: Remote Patient Monitoring; CGM: Continuous Glucose Monitoring; PHI: Personal Health Information.

References

1. Gandapur, Y.; Kianoush, S.; Kelli, H.M.; Misra, S.; Urrea, B.; Blaha, M.J.; Graham, G.; Marvel, F.A.; Martin, S.S. The role of mHealth for improving medication adherence in patients with cardiovascular disease: A systematic review. *Eur. Heart J.-Qual. Care Clin. Outcomes* **2016**, *2*, 237–244. [CrossRef] [PubMed]
2. Ming, L.C.; Untong, N.; Aliudin, N.A.; Osili, N.; Kifli, N.; Tan, C.S.; Goh, K.W.; Ng, P.W.; Al-Worafi, Y.M.; Lee, K.S.; et al. Mobile Health Apps on COVID-19 Launched in the Early Days of the Pandemic: Content Analysis and Review. *JMIR mHealth uHealth* **2020**, *8*, e19796. [CrossRef] [PubMed]
3. Shuren, J.; Patel, B.; Gottlieb, S. FDA Regulation of Mobile Medical Apps. *JAMA* **2018**, *320*, 337–338. [CrossRef] [PubMed]
4. Whitley, R.J.; Keutmann, H.T.; Ryan, R.J. Isolation and Characterization of the Subunits of Porcine Follicle-Stimulating Hormone. *Endocr. Res. Commun.* **1981**, *8*, 61–81. [CrossRef] [PubMed]
5. Van Kerkhof, L.W.M.; Van Der Laar, C.W.E.; De Jong, C.; Weda, M.; Hegger, I.; Blondon, K.; Fiordelli, M. Characterization of Apps and Other e-Tools for Medication Use: Insights Into Possible Benefits and Risks. *JMIR mHealth uHealth* **2016**, *4*, e34. [CrossRef]
6. Rowland, S.P.; Fitzgerald, J.E.; Holme, T.; Powell, J.; McGregor, A. What is the clinical value of mHealth for patients? *npj Digit. Med.* **2020**, *3*, 4. [CrossRef]
7. Tabi, K.; Randhawa, A.S.; Choi, F.; Mithani, Z.; Albers, F.; Schnieder, M.; Nikoo, M.; Vigo, D.; Jang, K.; Demlova, R.; et al. Mobile Apps for Medication Management: Review and Analysis. *JMIR mHealth uHealth* **2019**, *7*, e13608. [CrossRef]
8. Lomotey, R.K.; Deters, R. Mobile-Based Medical Data Accessibility in mHealth. In Proceedings of the 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, Oxford, UK, 8–11 April 2014; pp. 91–100. [CrossRef]
9. Patel, B.K.; Chapman, C.G.; Luo, N.; Woodruff, J.N.; Arora, V.M. Impact of Mobile Tablet Computers on Internal Medicine Resident Efficiency. *Arch. Intern. Med.* **2012**, *172*, 436–438. [CrossRef]
10. Yetisen, A.K.; Martinez-Hurtado, J.L.; Vasconcellos, F.D.C.; Simsekler, M.C.E.; Akram, M.S.; Lowe, C.R. The regulation of mobile medical applications. *Lab. Chip* **2014**, *14*, 833. [CrossRef]
11. Giansanti, D. The Role of the mHealth in the Fight against the Covid-19: Successes and Failures. *Healthcare* **2021**, *9*, 58. [CrossRef]
12. Asadzadeh, A.; Kalankesh, L.R. A scope of mobile health solutions in COVID-19 pandemics. *Inform. Med. Unlocked* **2021**, *23*, 100558. [CrossRef] [PubMed]
13. Lewis, T.L.; Wyatt, J.C. mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use. *J. Med. Internet Res.* **2014**, *16*, e210. [CrossRef] [PubMed]
14. Hanrahan, C.; Aungst, T.D.; Cole, S.; American Society of Health-System Pharmacists. Evaluating Mobile Medical Applications. 2014. Available online: http://ebooks.ashp.org/product/evaluating-mobile-medical-applications (accessed on 27 June 2021).
15. Wicks, P.; Chiauzzi, E. 'Trust but verify'—Five approaches to ensure safe medical apps. *BMC Med.* **2015**, *13*, 205. [CrossRef] [PubMed]

16. Vos, J.; Parker, C. Medical Device Regulation mHealth Policy and Position. 2012. Available online: https://www.gsma.com/iot/wp-content/uploads/2012/03/gsmamedicaldeviceregulationmhealthpolicyandposition.pdf (accessed on 1 February 2022).
17. Alon, N.; Stern, A.D.; Torous, J. Assessing the Food and Drug Administration's Risk-Based Framework for Software Precertification With Top Health Apps in the United States: Quality Improvement Study. *JMIR mHealth uHealth* **2020**, *8*, e20482. [CrossRef]
18. Leible, S.; Schlager, S.; Schubotz, M.; Gipp, B. A Review on Blockchain Technology and Blockchain Projects Fostering Open Science. *Front. Blockchain* **2019**, *2*, 16. [CrossRef]
19. Cai, W.; Wang, Z.; Ernst, J.B.; Hong, Z.; Feng, C.; Leung, V.C.M. Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access* **2018**, *6*, 53019–53033. [CrossRef]
20. Atzori, M. Blockchain technology and decentralized governance: Is the state still necessary? *J. Gov. Regul.* **2017**, *6*, 45–62. [CrossRef]
21. Hölbl, M.; Kompara, M.; Kamišalić, A.; Zlatolas, L.N. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
22. Gozman, D.; Liebenau, J.; Aste, T. A Case Study of Using Blockchain Technology in Regulatory Technology. *MIS Q. Exec.* **2020**, *19*, 19–37. [CrossRef]
23. Does Blockchain Mean an End to Regulatory Reporting as We Know it? *Deloitte*. Available online: https://www2.deloitte.com/uk/en/pages/financial-services/articles/does-blockchain-mean-an-end-to-regulatory-reporting.html (accessed on 1 September 2022).
24. Lohnari, T.; Patil, S.; Patil, S. Use of Mobile Applications in Healthcare: A Review. *Int. J. Eng. Res. Gen. Sci.* **2016**, *4*, 38–42.
25. Ventola, C.L. Mobile devices and apps for health care professionals: Uses and benefits. *Pharm. Ther.* **2014**, *39*, 356–364.
26. Mickan, S.; Tilson, J.K.; Atherton, H.; Roberts, N.W.; Heneghan, C.; Oh, H.; Wharrad, H. Evidence of Effectiveness of Health Care Professionals Using Handheld Computers: A Scoping Review of Systematic Reviews. *J. Med. Internet Res.* **2013**, *15*, e212. [CrossRef] [PubMed]
27. Murfin, M. Know Your Apps: An Evidence-Based Approach to Evaluation of Mobile Clinical Applications. *J. Physician Assist. Educ.* **2013**, *24*, 38–40. [CrossRef] [PubMed]
28. Mezarina, L.R.; Silva-Valencia, J.; Escobar-Agreda, S.; Herrera, D.H.E.; Egoavil, M.S.; Kuljich, M.M.; Inga-Berrospi, F.; Ronceros, S. Need for the Development of a Specific Regulatory Framework for Evaluation of Mobile Health Apps in Peru: Systematic Search on App Stores and Content Analysis. *JMIR mHealth uHealth* **2020**, *8*, e16753. [CrossRef] [PubMed]
29. Akbar, S.; Coiera, E.; Magrabi, F. Safety concerns with consumer-facing mobile health applications and their consequences: A scoping review. *J. Am. Med. Inform. Assoc.* **2020**, *27*, 330–340. [CrossRef]
30. Pandey, A.; Hasan, S.; Dubey, D.; Sarangi, S. Smartphone Apps as a Source of Cancer Information: Changing Trends in Health Information-Seeking Behavior. *J. Cancer Educ.* **2013**, *28*, 138–142. [CrossRef]
31. Haffey, F.; Brady, R.R.W.; Maxwell, S. A Comparison of the Reliability of Smartphone Apps for Opioid Conversion. *Drug Saf.* **2013**, *36*, 111–117. [CrossRef]
32. Fernandez-Luque, L.; Labarta, J.I.; Palmer, E.; Koledova, E. Content Analysis of Apps for Growth Monitoring and Growth Hormone Treatment: Systematic Search in the Android App Store. *JMIR mHealth uHealth* **2020**, *8*, e16208. [CrossRef]
33. Aljedaani, B.; Babar, M.A. Challenges With Developing Secure Mobile Health Applications: Systematic Review. *JMIR mHealth uHealth* **2021**, *9*, e15654. [CrossRef]
34. Cortez, N.G.; Cohen, I.G.; Kesselheim, A.S. FDA Regulation of Mobile Health Technologies. *N. Engl. J. Med.* **2014**, *371*, 372–379. [CrossRef]
35. Policy for Device Software Functions and Mobile Medical Applications, Rockville. Available online: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications (accessed on 1 September 2022).
36. Leeming, G.; Cunningham, J.; Ainsworth, J. A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. *Front. Med.* **2019**, *6*, 171. [CrossRef] [PubMed]
37. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
38. Huang, X.; Chen, H.S.; Jarrell, J.T.; A Carpenter, K.; Cohen, D.S. Blockchain in Healthcare: A Patient-Centered Model. *Biomed. J. Sci. Tech. Res.* **2019**, *20*, 15017–15022. [CrossRef]
39. Charles, W.; Marler, N.; Long, L.; Manion, S. Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research. *Front. Blockchain* **2019**, *2*, 18. [CrossRef]
40. Sanchez-Gomez, N.; Torres-Valderrama, J.; Garcia-Garcia, J.A.; Gutierrez, J.J.; Escalona, M.J. Model-Based Software Design and Testing in Blockchain Smart Contracts: A Systematic Literature Review. *IEEE Access* **2020**, *8*, 164556–164569. [CrossRef]
41. Górski, T. The $k + 1$ Symmetric Test Pattern for Smart Contracts. *Symmetry* **2022**, *14*, 1686. [CrossRef]
42. Han, J.; Zhang, Y.; Liu, J.; Li, Z.; Xian, M.; Wang, H.; Mao, F.; Chen, Y. A Blockchain-Based and SGX-Enabled Access Control Framework for IoT. *Electronics* **2022**, *11*, 2710. [CrossRef]
43. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. [CrossRef]
44. Rauchs, M.; Glidden, A.; Gordon, B.; Pieters, G.C.; Recanatini, M.; Rostand, F.; Vagneur, K.; Zhang, B.Z. Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electron. J.* **2018**. [CrossRef]
45. Santos, J.A.; Inácio, P.R.M.; Silva, B.M.C. Towards the Use of Blockchain in Mobile Health Services and Applications. *J. Med. Syst.* **2021**, *45*, 17. [CrossRef]
46. Taralunga, D.; Florea, B. A Blockchain-Enabled Framework for mHealth Systems. *Sensors* **2021**, *21*, 2828. [CrossRef] [PubMed]
47. Chen, Y.; Richter, J.I.; Patel, P.C. Decentralized Governance of Digital Platforms. *J. Manag.* **2021**, *47*, 1305–1337. [CrossRef]

48. Falazi, G.; Breitenbücher, U.; Daniel, F.; Lamparelli, A.; Leymann, F.; Yussupov, V. Smart Contract Invocation Protocol (SCIP): A Protocol for the Uniform Integration of Heterogeneous Blockchain Smart Contracts. In *Advanced Information Systems Engineering*; Dustdar, S., Yu, E., Salinesi, C., Rieu, D., Pant, V., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 12127, pp. 134–149. [CrossRef]
49. Azzolini, D.; Riguzzi, F.; Lamma, E. Studying Transaction Fees in the Bitcoin Blockchain with Probabilistic Logic Programming. *Information* **2019**, *10*, 335. [CrossRef]
50. Wykes, T.; Schueller, S. Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces. *J. Med. Internet Res.* **2019**, *21*, e12390. [CrossRef] [PubMed]
51. Zubaydi, F.; Saleh, A.; Aloul, F.; Sagahyroon, A. Security of mobile health (mHealth) systems. In Proceedings of the 2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE), Belgrade, Serbia, 2–4 November 2015; pp. 1–5. [CrossRef]
52. Jones, M.; Johnson, M.; Shervey, M.; Dudley, J.T.; Zimmerman, N. Privacy-Preserving Methods for Feature Engineering Using Blockchain: Review, Evaluation, and Proof of Concept. *J. Med. Internet Res.* **2019**, *21*, e13600. [CrossRef] [PubMed]
53. Marbouh, D.; Simsekler, M.C.E.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain-based Incident Reporting System for Patient Safety and Quality in Healthcare. In *Trust Models for Next-Generation Blockchain Ecosystems*; ur Rehman, M.H., Svetinovic, D., Salah, K., Damiani, E., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 167–190. [CrossRef]
54. Gurupur, V.P.; Wan, T.T.H. Challenges in implementing mHealth interventions: A technical perspective. *mHealth* **2017**, *3*, 32. [CrossRef] [PubMed]
55. Wong, P.-M.; Sinha, S.R.K.; Chui, C.-K. Blockchain in manufacturing quality control: A computer simulation study. *PLoS ONE* **2021**, *16*, e0247925. [CrossRef]
56. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A Blockchain-Based Supply Chain Quality Management Framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.
57. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
58. Alam, T. mHealth Communication Framework Using Blockchain and IoT Technologies. *Math. Comput. Sci.* **2020**, preprint. [CrossRef]
59. Jusoh, S. A Survey on Trend, Opportunities and Challenges of mHealth Apps. *Int. J. Interact. Mob. Technol. IJIM* **2017**, *11*, 73. [CrossRef]
60. Ozdayi, M.S.; Kantarcioglu, M.; Malin, B. Leveraging blockchain for immutable logging and querying across multiple sites. *BMC Med. Genom.* **2020**, *13*, 82. [CrossRef] [PubMed]
61. Yun, Y. The Influence of Blockchain Technology on Fraud and Fake Protection. *OUR J. ODU Undergrad. Res. J.* **2020**, *7*, 8. [CrossRef]
62. Pane, J.; Verhamme, K.M.; Shrum, L.; Rebollo, I.; Sturkenboom, M.C. Blockchain technology applications to postmarket surveillance of medical devices. *Expert Rev. Med. Devices* **2020**, *17*, 1123–1132. [CrossRef] [PubMed]
63. Bhutkar, G.; Karande, J.; Dhore, M. Major Challenges with Mobile Healthcare Applications. *Br. J. Healthc. Comput. Inf. Manag.* **2009**.
64. Motohashi, T.; Hirano, T.; Okumura, K.; Kashiyama, M.; Ichikawa, D.; Ueno, T. Secure and Scalable mHealth Data Management Using Blockchain Combined With Client Hashchain: System Design and Validation. *J. Med. Internet Res.* **2019**, *21*, e13385. [CrossRef]
65. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR mHealth uHealth* **2017**, *5*, e111. [CrossRef]
66. Ahmed, W.; Di, W.; Mukathe, D. A Blockchain-Enabled Incentive Trust Management with Threshold Ring Signature Scheme for Traffic Event Validation in VANETs. *Sensors* **2022**, *22*, 6715. [CrossRef]
67. Górski, T. The 1+5 Architectural Views Model in Designing Blockchain and IT System Integration Solutions. *Symmetry* **2021**, *13*, 2000. [CrossRef]
68. Demidowich, A.P.; Bloomgarden, Z.; Lu, K.; Tamler, R. An evaluation of diabetes self-management applications for Android smartphones. *J. Telemed. Telecare* **2012**, *18*, 235–238. [CrossRef]
69. Cichosz, S.L.; Stausholm, M.; Kronborg, T.; Vestergaard, P.; Hejlesen, O. How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept. *J. Diabetes Sci. Technol.* **2018**, *13*, 248–253. [CrossRef]
70. Cichosz, S.L.; Johansen, M.D.; Hejlesen, O. Toward Big Data Analytics. *J. Diabetes Sci. Technol.* **2015**, *10*, 27–34. [CrossRef] [PubMed]
71. Doyle-Delgado, K.; Chamberlain, J.J. Use of Diabetes-Related Applications and Digital Health Tools by People With Diabetes and Their Health Care Providers: Review of Predictive Models in Management of Diabetes and Its Complications. *Clin. Diabetes* **2020**, *38*, 449–461. [CrossRef] [PubMed]
72. Drincic, A.; Prahalad, P.; Greenwood, D.; Klonoff, D.C. Evidence-based Mobile Medical Applications in Diabetes. *Endocrinol. Metab. Clin. N. Am.* **2016**, *45*, 943–965. [CrossRef] [PubMed]
73. Fleming, G.A.; Petrie, J.R.; Bergenstal, R.M.; Holl, R.W.; Peters, A.L.; Heinemann, L. Diabetes Digital App Technology: Benefits, Challenges, and Recommendations. A Consensus Report by the European Association for the Study of Diabetes (EASD) and the American Diabetes Association (ADA) Diabetes Technology Working Group. *Diabetes Care* **2020**, *43*, 250–260. [CrossRef] [PubMed]
74. Kaufman, N.; Khurana, I. Using Digital Health Technology to Prevent and Treat Diabetes. *Diabetes Technol. Ther.* **2016**, *18*, S-56–S-68. [CrossRef] [PubMed]
75. Huckvale, K.; Adomaviciute, S.; Prieto, J.T.; Leow, M.K.-S.; Car, J. Smartphone apps for calculating insulin dose: A systematic assessment. *BMC Med.* **2015**, *13*, 106. [CrossRef]
76. Roncero, A.P.; Marques, G.; Sainz-De-Abajo, B.; Martín-Rodríguez, F.; Vegas, C.D.P.; Garcia-Zapirain, B.; de la Torre-Díez, I. Mobile Health Apps for Medical Emergencies: Systematic Review. *JMIR mHealth uHealth* **2020**, *8*, e18513. [CrossRef]

77. Hasselgren, A.; Wan, P.K.; Horn, M.; Kralevska, K.; Gligoroski, D. GDPR Compliance for Blockchain Applications in Healthcare. *arXiv* **2020**, arXiv:2009.12913.
78. Uddin, M.; Salah, K.; Jayaraman, R.; Pesic, S.; Ellahham, S. Blockchain for drug traceability: Architectures and open challenges. *Health Inform. J.* **2021**, *27*, 146045822110112. [CrossRef]
79. Sharma, A.; Kaur, S.; Singh, M. A comprehensive review on blockchain and Internet of Things in healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333. [CrossRef]
80. Suripeddi, M.K.S.; Purandare, P. Blockchain and GDPR—A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing. *J. Phys. Conf. Ser.* **2021**, *1964*, 042005. [CrossRef]
81. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2021**, *34*, 11475–11490. [CrossRef]
82. Mazlan, A.A.; Daud, S.M.; Sam, S.M.; Abas, H.; Rasid, S.Z.A.; Yusof, M.F. Scalability Challenges in Healthcare Blockchain System—A Systematic Review. *IEEE Access* **2020**, *8*, 23663–23673. [CrossRef]
83. Kaur, G.; Gandhi, C. Scalability in Blockchain: Challenges and Solutions. In *Handbook of Research on Blockchain Technology*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 373–406. [CrossRef]
84. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M. Blockchain for Waste Management in Smart Cities: A Survey. *IEEE Access* **2021**, *9*, 131520–131541. [CrossRef]
85. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]
86. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
87. Macdonald, M.; Liu-Thorrold, L.; Julien, R. The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin. *Work. Pap.* **2017**, 1–18. [CrossRef]
88. Kuo, T.-T.; Rojas, H.Z.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc. JAMIA* **2019**, *26*, 462–478. [CrossRef]
89. Chowdhury, M.J.M.; Ferdous, S.; Biswas, K.; Chowdhury, N.; Kayes, A.S.M.; Alazab, M.; Watters, P. A Comparative Analysis of Distributed Ledger Technology Platforms. *IEEE Access* **2019**, *7*, 167930–167943. [CrossRef]
90. Suhail, S.; Hussain, R.; Jurdak, R.; Oracevic, A.; Salah, K.; Hong, C.S.; Matulevičius, R. Blockchain-Based Digital Twins: Research Trends, Issues, and Future Challenges. *ACM Comput. Surv.* **2021**, *54*, 1–34. [CrossRef]