Universidad de Valparaíso
CHILE
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA CIVIL BIOMÉDICA

FACTIBILIDAD DE DESARROLLAR SISTEMAS DE IoMT PARA PACIENTES POSTRADOS EN CASA HACIENDO USO DE TECNOLOGÍA BLOCKCHAIN PARA LA SEGURIDAD DE LOS DATOS Y ESTÁNDAR FHIR PARA EL INTERCAMBIO DE INFORMACIÓN

VICTORIA BELÉN UMAÑA GONZÁLEZ

Trabajo para optar al título de

Ingeniero Biomédico

Profesor Guía:

Cesar Galindo

Agosto - 2021

Valparaíso – Chile

Resumen

Objetivo: Se realizó una revisión sistemática con el objetivo de identificar la posibilidad de implementar IoMT en conjunto con la tecnología Blockchain y el estándar FHIR, con tal de garantizar la seguridad y privacidad de los datos, así como el intercambio efectivo de información.
Método: Se utilizó la metodología PRISMA para la búsqueda de los artículos en dos bases de datos, usando los conceptos de búsqueda “IoT”, “IoMT”, “Blockchain” y “FHIR”. Además, de la inclusión de unos artículos de otras fuentes para complementar la búsqueda.
Resultados: La búsqueda arrojó un total de 2547 artículos, de los cuales, tras eliminar duplicados, aplicar los criterios de exclusión, y la eliminación post lectura, finalmente se analizaron un total de 17 artículos. Para cada artículo se identificaron los conceptos de interés y los métodos utilizados, así como también las limitaciones o brechas declaradas por los autores.
Discusión: Se observó un gran número de investigaciones con respecto a la aplicación de IoMT, pero este número se redujo al momento de considerar los aspectos de seguridad y privacidad de los datos. La falta de interoperabilidad a causa de la heterogeneidad de los datos parece ser uno de los principales problemas en los sistemas de información en salud.
Conclusión: A pesar de hallar un resultado que incluyera la combinación de las tecnologías investigadas en esta revisión sistemática, esta se encuentra en una etapa inicial, siendo necesario continuar profundizando en el tema realizando más investigaciones y estudios.

Palabras claves: *IoT, IoMT, Blockchain, FHIR.*

TABLA DE CONTENIDO

Factibilidad de desarrollar sistemas de IoMT para pacientes postrados en casa haciendo uso de tecnología Blockchain para la seguridad de los datos y estándar FHIR para el intercambio de información

Victoria Belén Umaña González
Escuela de Ingeniería Biomédica
Facultad de Ingeniería, Universidad de Valparaíso, Chile

Palabras clave: *IoT, IoMT, Blockchain, FHIR.*

1. INTRODUCCIÓN

Con la llegada de la tecnología 5G en las redes se verá impulsado el crecimiento de las IoT *(Internet of Things)* y otras aplicaciones de automatización inteligente, esto gracias a su rápida conexión y baja latencia que presenta [1]. En este sentido, es importante el desarrollo de las IoMT *(Internet of Medical Things)* con el fin de proveer sistemas que aporten a la salud de la comunidad.

En Chile, unas de las mayores preocupaciones son los pacientes postrados en casa. La situación de postración se puede deber a varios motivos, como a causa de un accidente, enfermedad o bien debido a la edad avanzada de la persona. La mayoría de los pacientes postrados son de la tercera edad [2], ya que, con la mejora en las tecnologías y la calidad de vida, se ha visto un aumento en la esperanza de vida de la población lo que se traduce en una mayor prevalencia de patologías que postran a los pacientes.

La utilización de IoMT en los hogares de pacientes postrados podría permitir recopilar información, hacer seguimiento y mejorar la calidad de vida de los pacientes. Sin embargo, para implementar estas tecnologías es importante integrar la información manteniendo al mismo tiempo la confidencialidad de los datos, es decir, que esta información sea accesible sólo para personas debidamente autorizadas, ya que se tratan de datos sensibles, tal cómo se definen en la Ley N °19628, artículo 2, letra g. [3].

A causa de la irrupción de las IoMT es que se deberá garantizar el manejo adecuado de este volumen de información asegurando que la comunicación sea segura, robusta y trazable. Debido a esto es que se han estudiado estructuras y tecnologías de manejo de datos como blockchain para cumplir con tal objetivo. Sin embargo, el uso de esta tecnología en salud conlleva un problema al momento de realizar el intercambio de información, ya que las cadenas de datos son tan largas que se vuelven lentas de computar, por lo que se ha visto la posibilidad de combinar esta tecnología con otro tipo de estándares como el estándar HL7 FHIR para lograr una mejor comunicación e integración de la información.

Por lo tanto, en esta revisión sistemática se busca recolectar evidencias presentes a la fecha de la aplicación o intentos de desarrollar tecnología IoMT para pacientes postrados en sus domicilios, utilizando tecnología Blockchain para la seguridad de los datos y el estándar FHIR para su integración, teniendo en cuenta los métodos probados y los resultados obtenidos.

Lo explicado anteriormente nos motiva debido a que mediante esta investigación se esperan encontrar los siguientes resultados en esta revisión sistemática.

- Aplicación de blockchain a IoMT y los métodos utilizados y las dificultades que pudiera presentar.

- Identificación de métodos y resultados presentes en estudios, investigaciones o desarrollos orientados hacia la aplicación de blockchain y FHIR en particular.
- Brechas tecnológicas para poder implementar IoMT de manera masiva haciendo uso de estándares de información actuales.

Esto con el fin de responder a los siguientes objetivos:

- Determinar si efectivamente los estándares o mecanismos de comunicación de última generación pueden convivir en salud y en este caso particular, mejorar la calidad de vida de los pacientes postrados.
- Determinar cuán simple o difícil sería para el país adoptar estas tecnologías IoMT.
- Determinar qué brechas existen para llevar a cabo la implementación de las tecnologías IoMT en el país.

Para llevar a cabo lo antes mencionado, se comenzará en la sección 2 por definir algunos conceptos que se utilizarán a lo largo de esta revisión, para luego en la sección 3 establecer la metodología de búsqueda y selección de los artículos con los que se obtendrá la información relacionada con el tema de interés, entonces continuar en la sección 4 con la presentación de los resultados obtenidos al finalizar la revisión de literatura, para terminar en la sección 5 con una discusión sobre los resultados y concluir con una respuesta a la pregunta planteada en esta revisión en base a los resultados obtenidos.

2. MARCO TEÓRICO

Dado lo emergente de las tecnologías abordadas e investigadas en esta revisión de literatura, para lograr un mejor desarrollo de esta y con el fin de otorgar una mejor comprensión del tema, el marco teórico será abordado mediante la definición de los conceptos más relevantes, los cuales serían precisamente estas tecnologías, IoMT, Blockchain y el estándar HL7 FHIR, que por lo novedoso de ellas puede que no estén en el conocimiento y/o manejo de todos los lectores. Además de sus definiciones, también se consideró una breve explicación de sus características, sus arquitecturas y tecnologías.

2.1 INTERNET DE LAS COSAS MÉDICAS (IoMT)

La tecnología IoT trata de una infraestructura global que conecta a Internet distintos dispositivos y aplicaciones, capaces de procesar, comunicar y almacenar datos captados del mundo físico [4]. A partir de la tecnología IoT se deriva el término IoMT, enfocado en el área médica y se refiere a un conjunto de sistemas de atención sanitaria que permite la transmisión de datos sanitarios entre dispositivos inteligentes para apoyar de forma remota el trabajo de los médicos, proveedores de atención de salud y centros de pruebas médicas y así almacenar e intercambiar estos de forma segura, además de la posibilidad de otorgar servicios y asistencia médica en tiempo real [5].

En IoMT, las tecnologías de IoT como la identificación por radiofrecuencia, la tecnología de sensores y la tecnología de posicionamiento, se combinan con terminales móviles, comunicaciones de red y otros dispositivos para lograr la digitalización, automatización y sistemas sanitarios inteligentes [6].

Los dispositivos sanitarios que componen IoMT se pueden clasificar según su tipo en [7] (ver figura 1):

- Dispositivos médicos fijos
- Dispositivos médicos integrados
- Dispositivos médicos portátiles
- Dispositivos portátiles de control de la salud

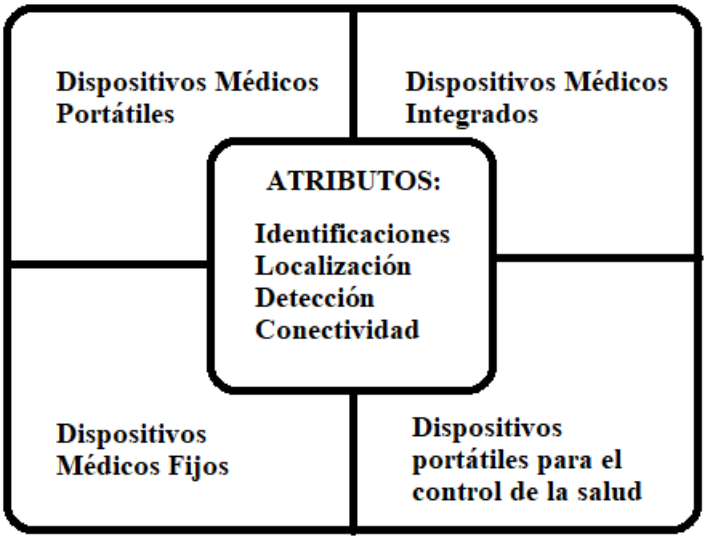

Fig.1 Dispositivos IoMT. Fuente [7]

Dentro de este último grupo, los sensores médicos portátiles son clave en la obtención de datos de signos vitales de los pacientes.

2.1.1 ARQUITECTURA TRADICIONAL DE IoMT

El IoMT tradicional sigue la arquitectura general de tres niveles de la aplicación de IoT como se observa en figura 2, estos niveles son [6], [8]:

1. El nivel local o capa de percepción**,** que se divide en dos subcapas:
   i) La subcapa de adquisición de datos donde se completa la percepción y la identificación de los nodos en el IoMT y también se recoge la información de los datos de las personas y cosas. Utiliza métodos de adquisición de señales para transmitir todas las personas y objetos que participan en la red en nodos de sistemas ciberfísicos (CPS) que son fáciles de identificar. Los nodos del IoT se dividen en: CPS pasivos, CPS activos y CPS de internet.
   ii) La subcapa de acceso a los datos utiliza métodos de acceso para conectar los datos recogidos por la adquisición de datos a la capa de red mediante tecnología de transmisión de datos a corta distancia. Los métodos de acceso utilizados van a depender de las características del IoMT y las necesidades de los objetos.

2. El nivel de acceso o capa de red, que se divide en dos subcapas:
   i) Capa de transmisión de red, esta es la red troncal del IoMT y utiliza la red de comunicaciones móviles, Internet y otras redes especiales para transmitir la información de los datos adquiridos en tiempo real y de manera precisa y fiable.
   ii) Capa de servicio, esta capa integra las redes heterogéneas, los distintos formatos de datos, descripciones y otras informaciones. Además, construye una plataforma de soporte de servicios, la cual da una interfaz abierta para varios servicios en la capa de aplicación.

3. El nivel central o capa de aplicación: Se divide en las siguientes capas:
   i) Capa de aplicación de la información médica, la que incluye todo lo que respecta a la gestión de información.
   ii) Capa de aplicación de toma de decisiones de información médica, que incluye todo lo que respecta al análisis de la información.

Las principales tecnologías utilizadas en el IoMT tradicional son la RFID para identificar objetos, leer y escribir los datos pertinentes, almacenar información del objeto y recopilar datos de los signos vitales; la red de sensores inalámbricos (WSN) que cumple con funciones de adquisición, procesamiento y transmisión de datos, también puede monitorizar, percibir y recolectar información de diferentes entornos u objetos en tiempo real, y enviar la información procesada por vía inalámbrica; y el middleware, el cual realiza el papel de intermediario y es capaz de satisfacer las necesidades de aplicaciones, soportar la computación distribuida y a los dispositivos de sensores, además, puede también realizar la estandarización de diferentes entornos de aplicación y la comunicación de datos entre sistemas de aplicación [6].

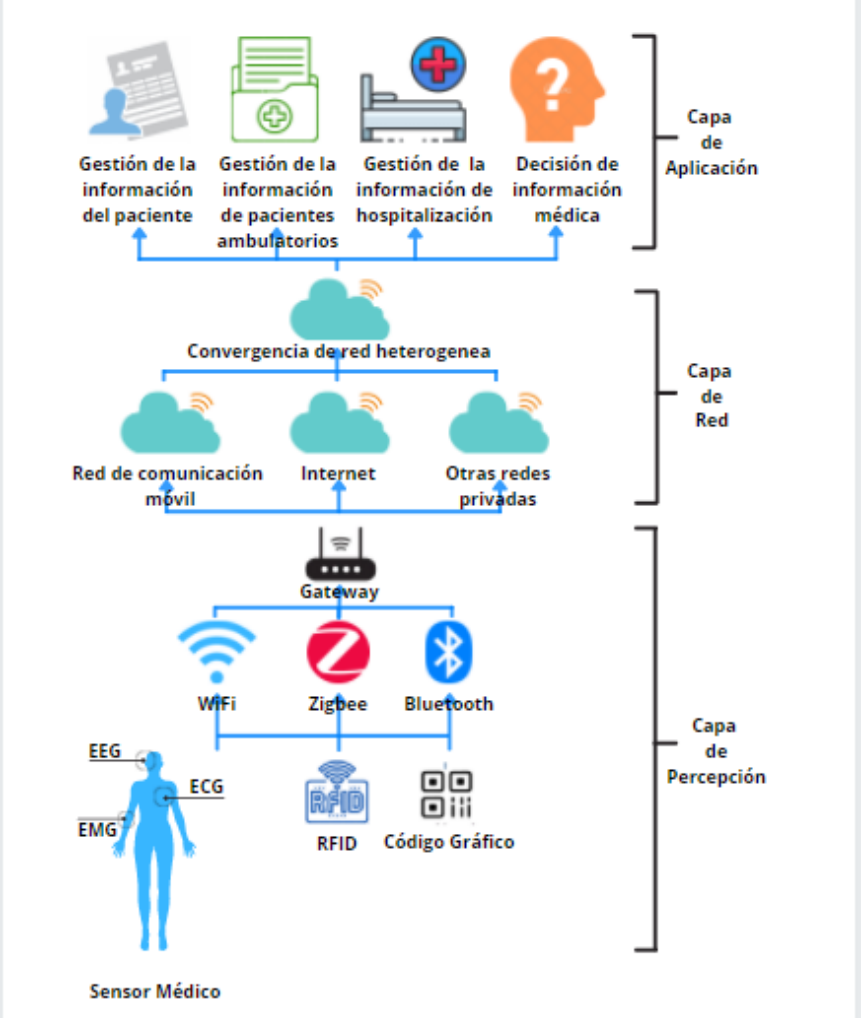

Fig. 2. Arquitectura IoMT. Fuente [6].

2.1.2 ARQUITECTURA TRADICIONAL DE IoMT

Arquitectura de IoMT en la nube

La arquitectura del IoMT combinada con la computación en la nube consta de tres niveles [6]:

1) **Capa de gestión de servicios**, esta incluye un sistema completo de monitorización, así como funciones de gestión múltiple, con el objetivo de garantizar que todo el sistema de información de salud funcione de forma segura y estable
2) **Capa de servicios médicos**, esta capa de divide en 3 subcapas:
   - La capa de infraestructura médica, que proporciona los recursos y servicios informáticos, de almacenamiento y de red.
   - La capa de plataforma médica, otorga una plataforma básica y soporte técnico para los desarrolladores del sistema de información de salud.
   - La capa de software médico, realiza la liberación y la interfaz del software funcional del sistema de información de salud para los usuarios finales.
3) **Capa de usuario**, en el caso de los médicos permite rastrear y obtener información de los pacientes, sus tratamientos, entre otros, en tiempo real, mientras que a los pacientes les permite elegir una institución médica para tratarse según sus condiciones.

Las principales tecnologías utilizadas por IoMT en la nube son 1) Computación en la nube, la cual da ciertas ventajas al IoMT en comparación a la red tradicional en cuanto a recursos, fiabilidad y rendimiento; 2) Big Data, que permite la recopilación, el preprocesamiento, el almacenamiento, y el análisis y minería de los datos; 3) Inteligencia Artificial (IA), esta incluye el aprendizaje automático (ML), el procesamiento del lenguaje natural (NPL), la robótica, la visión por computador y el sistema experto, siendo una de las más importantes el ML, ya que incluye este incluye el *Deep Learning* (DL) [6].

Entre algunas de las múltiples aplicaciones de IoMT se encuentran las siguientes [5], [9]–[12]:

- Medición de parámetros sanitarios en tiempo real.
- Proporcionar tratamientos automatizados basados en mediciones realizadas por sensores.
- Posibilidad de autogestión de su enfermedad por pacientes crónicos.
- Monitoreo de condiciones fisiológicas y parámetros de salud vitales.
- Almacenamiento e intercambio de datos.
- Servicio y asistencia médica en tiempo real.
- Seguimiento del nivel de forma física.

2.2 BLOCKCHAIN

Blockchain es un libro de contabilidad compartido y distribuido que ayuda con el proceso de registro de las transacciones y el seguimiento de los activos en una red [13]. La cadena de bloques consta de una lista de registros ordenados cronológicamente por marca de tiempo discretas y es administrada por una red distribuida, lo que favorece la integridad de los datos. Cada bloque puede tener múltiples transacciones y se conecta con el bloque frontal a través de un hash criptográfico. Generalmente un bloque tiene una carga útil, una marca de tiempo y una clase especial de funciones hash calculadas por los bloques anteriores. El primer bloque es llamado Génesis [7]. Las transacciones de cada bloque se

forman como un árbol de Merkel y cada valor de transacción (hoja) se verifica con la raíz conocida. Sólo la raíz se registra en el bloque [12], [14].

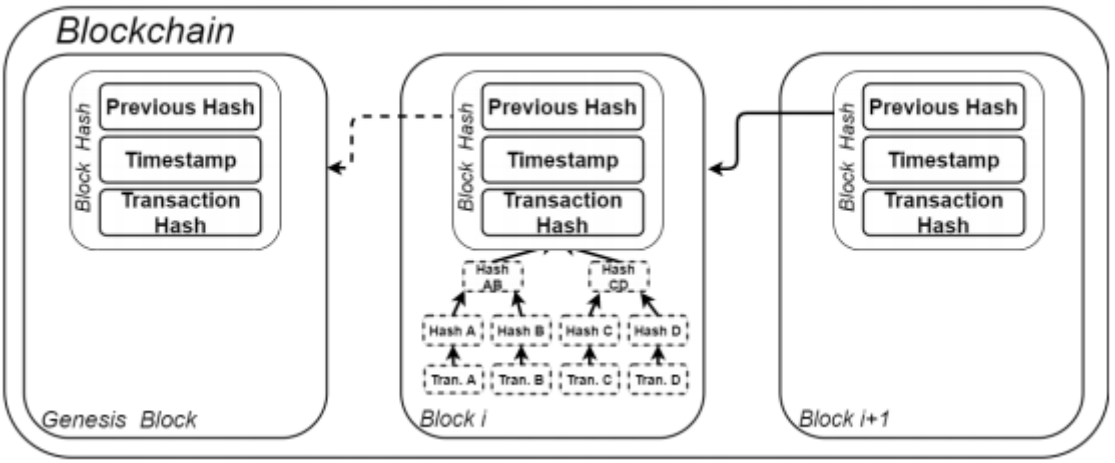

Fig. 3 Estructura básica de Blockchain [12].

Existen tres tipos de cadenas de bloques dependiendo de quién puede acceder, escribir y leer la información [12], [14]:

- Las cadenas públicas sin permiso, donde cualquiera puede unirse a la cadena durante el proceso de consenso, leer y escribir información. Un ejemplo de ellas son Bitcoin y Ethereum.
- Las cadenas privadas, generalmente son administradas por una autoridad central y ningún participante tiene permiso de lectura.
- Las cadenas de consorcio, donde las decisiones de consenso son tomadas por un grupo definido, previo registro de los participantes. Para validar un bloque requiere un mínimo de miembros.

Para validar y actualizar bloques, existen protocolos de consenso distribuido [12], [14], [15]:

1) Prueba de trabajo (*Proof of Work*, PoW), donde un bloque puede ser validado por un nodo de red si el participante prueba que se han gastado una cantidad predefinida de recursos computacionales.
2) Prueba de Participación (PoS), se logra el consenso al pedir a los usuarios que apuesten una cantidad de sus tokens para aumentar la posibilidad de ser seleccionados para aceptar un bloque de transacciones y obtener recompensas.
3) Prueba de tiempo transcurrido, similar a la PoW, pero reemplaza la demanda de un proceso intensivo de minería con un sistema de temporizador aleatorio.
4) Práctica de tolerancia a fallas bizantinas (PBFT): es una característica de una red distribuida para llegar a un consenso, aún si los nodos en la red no responden o no lo hacen incorrectamente. Entonces se utiliza una decisión colectiva con el fin de reducir la influencia de los nodos defectuosos.

Tras ser validado el hash del nuevo bloque, este es agregado a la cadena, en este punto la transacción no puede ser alterada, ya que queda protegido contra manipulación mediante criptografía [12], [15].

Los nodos de la cadena de bloques, llamados también mineros, pueden tener diferentes roles [12], [14]:

- Nodo ligero, que mantiene sólo el encabezado de cada bloque en su almacenamiento local.
- Nodo completo, almacena una copia completa y actualizada de la cadena de bloques, y verifican de forma autónoma las transacciones sin referencia externa.
- Nodos de consenso, estos influyen en el estado de la cadena de bloques publicando nuevos bloques.

Por otro lado, hay aplicaciones de Blockchain en que se permiten contratos inteligentes [12]. Un contrato inteligente, es un conjunto de líneas de código autoejecutables y que contienen reglas pre especificadas las cuales deben cumplirse durante una transacción de la cadena de bloques.

Entre las principales aplicaciones de Blockchain en el área de salud se encuentran [12]:

- Registro, almacenamiento e intercambio de datos sensibles
- Recopilación y almacenamiento a distancia de datos sanitarios
- Intercambio de información con fines clínicos, de estudio y/o administrativos.
- Gestión del acceso a los datos sensibles de los usuarios y el HCE.
- Recopilar y compartir datos de sensores médicos con fines clínicos.
- Recopilación y almacenamiento de datos para diagnósticos automatizados.
- Compartir datos de salud entre establecimientos de salud.
- Gestión y almacenamiento de los datos de pacientes en un entorno de nube.
- Seguimiento del brote de enfermedades infecciosas.
- Recuperar información en el HCE.
- Toma de decisiones mediante la presentación de conocimientos.

También estas se pueden dividir en tres grandes clases, figura 4: 1) La gestión de Datos, 2) La gestión de la cadena de suministros y 3) IoMT y seguridad de los datos [16].

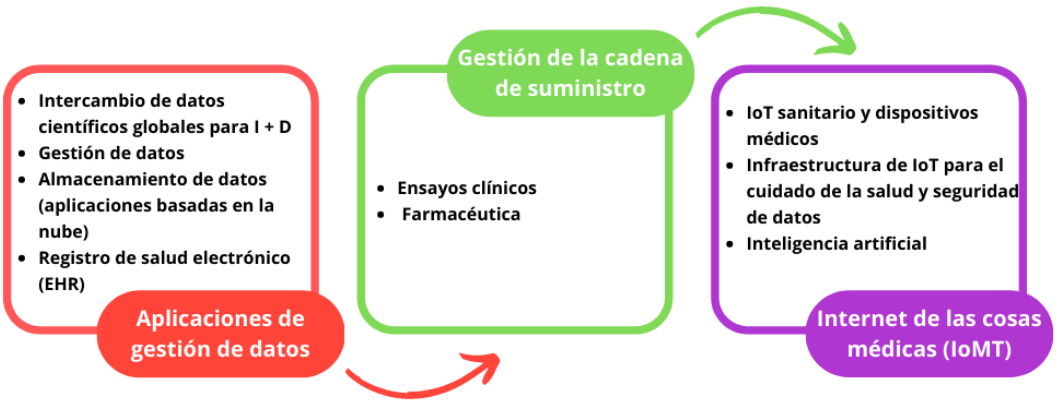

Fig. 4 Aplicaciones de salud basadas en Blockchain [16].

2.3 ESTÁNDAR HL7 FHIR

FHIR (*Fast Healthcare Interoperability Resources*) es un estándar desarrollado por HL7 que permite el intercambio de información para la prestación de asistencia sanitaria en una gran variedad de entornos. Es considerado como el marco de interoperabilidad de la información sanitaria de próxima

generación. Este se basa en recursos web y en adaptar prácticas RESTful para la prestación de servicios médicos integrados [4], [11].

Se fundamenta en “Recursos”, siendo estos la unidad básica para cualquier intercambio y definen los elementos de datos, las restricciones y las relaciones para los objetos más relevantes para la atención médica (como paciente, observación, entre otros) [17]. Sus características comunes incluyen una URL que identifica los metadatos comunes del recurso, un resumen XHTML legible, un conjunto de datos definidos, diferentes para cada tipo de recurso y un marco de extensibilidad que soporta variaciones en la atención médica. Las instancias de recursos de representan como XML, JSON, o RDF [4].

3. METODOLOGÍA

El interés de investigar sobre el desarrollo y aplicación de las tecnologías mencionadas anteriormente, es una forma de buscar acercar el sistema de salud chileno a la realidad de los sistemas de salud en países más desarrollados que tienen una alta automatización de los procesos de salud, como por ejemplo, Canadá, Australia, Corea o Finlandia, esperando como resultado determinar si es posible el desarrollo y combinación de estas tecnologías, así como también poder identificar las brechas existentes a nivel nacional para lograrlo y cómo se debería proceder para implementar esto y mejorar la calidad de atención del paciente y cuál sería el impacto en la salud del paciente.

El primer paso metodológico como inicio de la metodología consistió en hacer una búsqueda sistemática de documentos relacionados con el tema de interés establecido, haciendo uso de las bases de datos PubMed e IEEE. Para realizar la búsqueda se aplicaron los siguientes conceptos: IoT, IoMT, tecnología Blockchain y el estándar HL7 FHIR, teniendo por lo tanto los términos IoT, IoMT, Blockchain y FHIR como palabras claves de búsqueda.

El siguiente paso metodológico consistió en definir los criterios de inclusión y exclusión. Como criterios de inclusión, al tratarse de una tecnología relativamente reciente y que se va actualizando constantemente, se consideró un rango de búsqueda de 5 años, o sea, se incluyeron los artículos publicados desde el año 2016 en adelante. También se consideraron los artículos de *journals* y *magazines* tanto en idioma inglés como español.

Por otra parte, se excluyeron los documentos que fueran tesis, conferencias, documentos de compañías y revisiones sistemáticas para evitar redundancia. También todos los artículos publicados previo al año 2016 y en otro idioma que no fueran los ya mencionados, así como los artículos que no tuvieran información de interés a pesar de contener los términos utilizados en la búsqueda o que se alejaban mucho conceptualmente de la investigación realizada.

Para realizar la búsqueda en las bases de datos se utilizaron las siguientes expresiones de búsqueda:

- (IoMT OR IoT) AND (Blockchain OR FHIR).
- (IoMT OR IoT) AND (Blockchain AND FHIR).

Para realizar la búsqueda y filtrado de los documentos se utilizó el método PRISMA, en la Figura 1 se presenta el diagrama de flujo utilizado para el proceso de selección de los artículos que se incluirán en la revisión sistemática.

Luego, el siguiente paso metodológico fue establecer los criterios de análisis a considerar al momento de realizar la lectura del artículo completo y que datos o información extraer de ellos. Se consideraron los siguientes criterios de análisis.

- Exactitud o cercanía del tema del artículo con la pregunta de investigación, la cual se determinó al momento de revisar los resúmenes de cada documento.

- Conclusión y validación del tema propuesto en el documento analizado, en otras palabras, analizar cuál es la calidad de la evidencia presentada en el artículo, determinando cuál fue el diseño de estudio o la metodología utilizada en cada documento.
- Los conceptos de interés establecidos para realizar la revisión sistemática se encuentran presentes en el contenido del documento.
- Identificación de indicadores, tales como:
    - Grado de éxito alcanzado por las implementaciones documentadas.
    - Grado de cercanía respecto a la factibilidad que se probaron en los estudios.
    - Impacto causado por estas implementaciones en la comunidad.

Como último paso en la metodología, se establecieron los sesgos o riesgos en la información que se podrían presentar al realizar la búsqueda sistemática de literatura. Los principales sesgos que se consideraron fueron los siguientes:

- Lo novedoso de la tecnología puede hacer que la conclusión pierda objetividad.
- La información presente en los documentos puede ser parcial a causa de lo reciente de la tecnología.
- Es especulativo hablar del desarrollo de aplicaciones IoT o IoMT sin que la tecnología 5G se encuentre masivamente extendida.

4. RESULTADOS

4.1 SELECCIÓN DE ARTÍCULOS

Como ya se mencionó en la sección anterior, la selección de artículos se realizó según el método PRISMA. Entonces, luego de realizar la búsqueda en las bases de datos mencionadas en la sección de metodología, se consiguió un total 2625 artículos, a los cuales se le agregaron 4 artículos obtenidos de otras fuentes. De este primer resultado de búsqueda, se eliminaron 82 artículos que estaban duplicados, quedando un total 2547 artículos. En seguida, se procedió a aplicar los criterios de inclusión y exclusión previamente descritos, reduciéndose el número de artículos para analizar a un total de 111, tal como se observa en la figura 1. Entonces se prosiguió a leer los resúmenes para identificar los artículos en que el enfoque fuera similar o cercano al objetivo de la pregunta de interés de esta revisión sistemática.

Tras la lectura de los resúmenes se obtuvo un total de 21 artículos cumplían con el enfoque buscado, el resto de los artículos se enfocan en otra área o bien sólo se enfocan en la aplicación de IoMT a usos específicos de salud y no consideraban el aspecto de la seguridad de los datos, ni el uso de Blockchain o la integración de los datos de forma interoperable, o bien el uso de FHIR.
Al iniciar la lectura de los textos completos de los artículos se eliminaron dos artículos, ya que resultó imposible acceder a ellos gratuitamente.

Finalmente, después de realizar la lectura del texto completo, el número de artículos que cumplen con los criterios establecidos e incluyen los conceptos de interés de esta revisión sistemática corresponden a un total de 17 artículos.

4.2 IDENTIFICACIÓN DE FUENTES

De los artículos seleccionados se observó que la mayoría de ellos (a excepción de 3 artículos) aplicaban la tecnología Blockchain para la seguridad de los datos, con un método distinto de FHIR

para la integración de los datos, o bien, utilizaban FHIR, pero sin mencionar el concepto de Blockchain.

Para cada artículo se identificó el método utilizado para implementar el concepto de interés (Blockchain o FHIR), las limitaciones que presentaba su implementación y las brechas que expresaban para la implementación de aplicaciones IoMT. De los resultados, se observa que la mayoría de los artículos se enfocan en la aplicación de Blockchain a IoMT, y muy pocos a la aplicación de FHIR.

En base a los resultados observados, presentados en la tabla 1, se procedió a agrupar y analizar los artículos según el concepto aplicado y la metodología utilizada para su implementación.

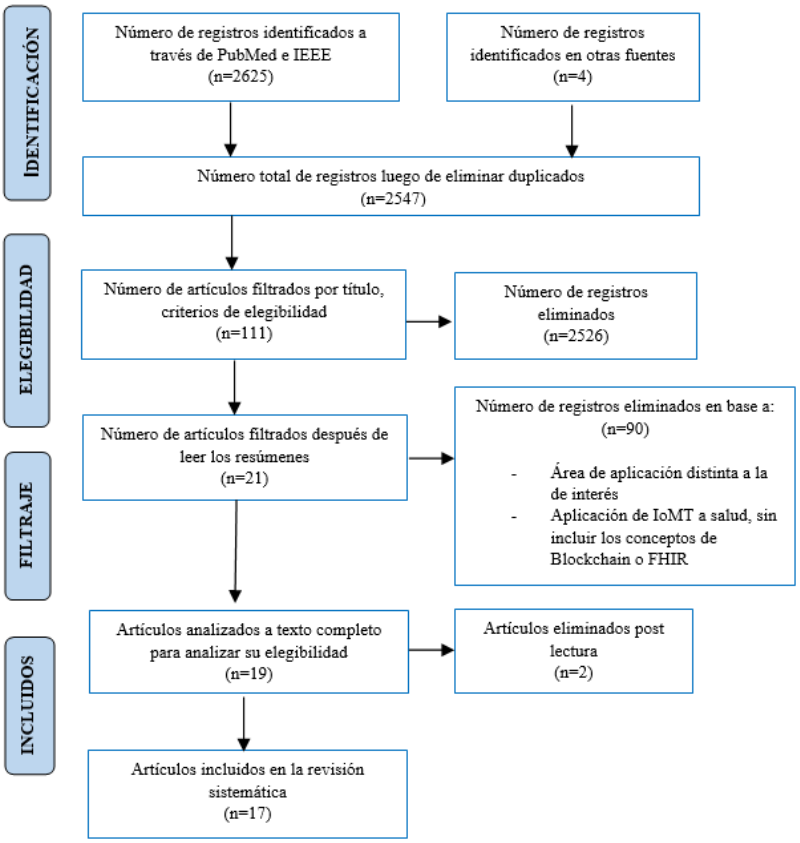

Fig. 5 Diagrama de flujo PRISMA, proceso de selección de los artículos para la revisión sistemática.

TABLA I
Identificación de fuentes según concepto y método implementado

Referencia	Año	Título	Concepto utilizado	Método implementado
Kim [9]	2017	*Development of parkinson patient generated data collection platform using FHIR and IoT devices.*	FHIR	Recolección de datos en formato FHIR para luego consultarlos mediante funciones API RESTful.
Griggs [10]	2018	*Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring*	Blockchain	Uso de contratos inteligentes basados en Blockchain de consorcio para registrar las transacciones de los sensores médicos de una WBAN.

Peng, [11]	2019	*Meaningful Integration of Data from Heterogeneous Health Services and Home Environment Based on Ontology.*	FHIR	Modelo que sigue el camino FHIR para aplicar tecnologías de la Web semántica y el modelo de recursos REST para integrar datos heterogéneos como recursos vinculados.
Dwivedi, [7]	2019	*A Decentralized Privacy-Preserving Healthcare Blockchain for IoT.*	Blockchain	Esquema ligero de firma en anillo para realizar transacciones anónimas, utilizando además doble cifrado de los datos y la técnica de intercambio de claves Diffie-Hellman.
Tripathi [18]	2020	*S2HS- A blockchain based approach for a smart healthcare system.*	Blockchain	Sistema de atención médica seguro e inteligente mediante el uso de Blockchain
Meng, [14]	2020	*Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks*	Blockchain	Presentan un esquema de autenticación de confianza basado en Blockchain y la inferencia bayesiana para proteger los MSN contra ataques internos
Dai, [19]	2020	*Blockchain-Enabled Internet of Medical Things to Combat COVID-19*	Blockchain	Proponen la integración de Blockchain con IoMT enfocado al COVID-19 incluyendo: el rastreo del origen de la pandemia, la cuarentena y distanciamiento social, el hospital inteligente, la procedencia de los datos médicos y la asistencia sanitaria a distancia y la telemedicina.
Garg [5]	2020	*BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment*	Blockchain	Plantean habilitar mediante Blockchain privado un protocolo seguro de claves autenticadas para el entorno IoMT.
Taralunga, [12]	2021	*A Blockchain-Enabled Framework for mHealth Systems*	Blockchain	Proponen la creación de una aplicación descentralizada de m-Health que monitorea los parámetros del paciente a través de sensores portátiles usando una cadena de bloques Ethereum privada, para así abordar los desafíos de seguridad, integridad y procedencia de los datos.
Ejaz, [8]	2021	*Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications*	Blockchain	Plantean la integración de Blockchain y la computación de borde con un enfoque en el impacto que esto tendría en la eficacia y eficiencia de los sistemas de monitoreo de salud remoto.
Zhang [15]	2018	*FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data*	FHIR, Blockchain	Presentan las consideraciones arquitectónicas para sistemas de intercambio de datos clínicos seguros y escalables basados en Blockchain, haciendo uso también de elementos de

				datos FHIR junto con un diseño basado en tokens.
Mavrogiorgou [1]	2019	*Internet of Medical Things (IoMT): Acquiring and Transforming Data into HL7 FHIR through 5G Network Slicing*	FHIR	Proponen una plataforma de extremo a extremo en el que los dispositivos IoMT para diferentes escenarios de aplicaciones de que se conectan por WiFi mediante el mecanismo de adquisición de datos propuesto, se adquieren los datos de estos dispositivos conectados y sus especificaciones de red para ser segmentados en diferentes cortes de red 5G mediante el mecanismo *Slicing Management*, atendiendo a los requerimientos de computación de los diferentes escenarios, además de hacer los datos interoperables a través de su traducción a HL7 FHIR.
Aileni [16]	2020	*IoMT: A Blockchain Perspective*	Blockchain	Analizan los beneficios de la implementación de IoMT, así como también las oportunidades que presenta el uso de Blockchain en salud.
Peterson [20]	2016	*A Blockchain-Based Approach to Health Information Exchange Networks*	Blockchain, FHIR	Describen un enfoque del uso de Blockchain y FHIR para el desarrollo de redes de intercambio de datos en salud.
1upHealth [21]	2021	*Blockchain FHIR Provenance*	Blockchain, FHIR	Desarrollo de una API FHIR combinada con el uso de Blockchain

Fuente: Elaboración propia

4.3 IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN PARA IoMT

La mayoría de los artículos encontrados en esta búsqueda ofrecen aplicaciones de Blockchain orientadas al área de la salud, sin embargo, a excepción de dos artículos no se encontraron otros que combinen la cadena de bloques junto con el estándar FHIR.

En [10] proponen un sistema de Blockchain orientado en el paciente usando contratos inteligentes modulares y personalizables para cada paciente y dispositivo, con tal de facilitar el análisis automático de los datos sanitarios adquiridos por dispositivos WBAN. El sistema utiliza las propiedades del libro mayor distribuido de la cadena de bloques para la autenticidad y la verificabilidad, manteniendo la privacidad mediante la gestión de consorcio con permiso y cuentas anónimas. En este sistema sólo se registran los sucesos de los eventos, sin embargo, no se almacena información médica en Blockchain o en los contratos inteligentes para cumplir con las disposiciones de HIPAA (*Health Insurance Portability and Accountability Act*). El sistema fue implementado en una cadena de bloques privada que usa el protocolo de Ethereum. Hacen una comparación entre el sistema propuesto y el sistema tradicional, logrando características tales como una seguridad equivalente, una mayor disponibilidad de los datos y tolerancia a fallos, inmutabilidad, trazabilidad, mayor velocidad en las transacciones, privacidad, anonimato y transparencia.

En [7] proponen un modelo de Blockchain, eliminando el concepto de PoW (*Proof of Work*) y dividiendo la red superpuesta en varios clústeres en lugar de una sola cadena de bloques, para hacerlo apto para dispositivos IoT. También presentan un esquema ligero de firma en anillo que preserva la

privacidad y que es adecuado para transacciones anónimas de los usuarios auténticos. Además, utiliza el doble cifrado de los datos mediante algoritmos de cifrado ligero (ARX) y esquemas de cifrado público. Para el intercambio seguro de claves a través de un canal público, utilizaron la técnica de intercambio de claves Diffie-Hellman. La implementación conjunta de estas técnicas puede garantizar la seguridad, privacidad y anonimato de los datos del usuario. En la evaluación del modelo propuesto se contemplaron los requisitos de confidencialidad, autenticación, control de usuario, integridad, disponibilidad y anonimato de los datos. También consideraron los posibles ataques (ataque de denegación de servicio, ataque de minería, ataque de almacenamiento y ataque de caída) a los que podría ser vulnerable el modelo propuesto y encontraron un margen de seguridad contra ellos.

En [18] proponen un sistema de atención médica seguro e inteligente (S2HS) mediante la implementación de Blockchain. La información y los datos son captados por sensores que se cifran mediante cadena de bloques y se almacenan de manera distribuida en la nube. A estos datos sólo accede una persona legítima con el consentimiento de los pacientes. Este sistema, a grandes rasgos lo componen sensores integrados en dispositivos IoT, los registros clínicos de los pacientes, el cifrado y estandarización de los datos y la información, el mecanismo de cadena de bloques y los usuarios finales. El modelo no se implementa, sólo se trata de un análisis conceptual.

En [14] presentan un esquema de administración de confianza basado en Blockchain y la inferencia bayesiana para proteger los MSN (*Medical Smartphone Network*) contra ataques internos, mejorando la precisión de detección de nodos internos maliciosos. La evaluación del sistema fue realizada en dos entornos médicos, bajo la condición de tráfico de red normal y la condición de adversario. Los resultados obtenidos mostraron que el esquema propuesto presenta un mejor rendimiento en comparación con el esquema original, pudiendo detectar nodos maliciosos de manera más rápida.

En [19] plantean la integración de Blockchain con IoMT enfocado particularmente al COVID-19, donde proponen soluciones desde cinco perspectivas: el rastreo del origen de la pandemia, la cuarentena y distanciamiento social, el hospital inteligente, la procedencia de los datos médicos y la asistencia sanitaria a distancia y la telemedicina. Además, mencionan retos a resolver en orientaciones futuras, tales como, la escalabilidad de Blockchain, *Deep Learning* e Inteligencia artificial fiable para IoMT.

En [5] proponen habilitar mediante Blockchain privado un protocolo seguro de claves autenticadas para el entorno IoMT. El esquema propuesto es llamado BAKMP-IoMT y considera ocho fases: 1) pre despliegue, 2) gestión de claves, 3) registro de usuarios, 4) inicio de sesión, 5) autenticación y acuerdo de claves, 6) construcción y adición de la cadena de bloques, 7) actualización de contraseñas y actualización biométrica y 8) adición dinámica de IMD (*Implantable Medical Device*). Para evaluar el esquema propuesto, realizaron un análisis de seguridad informal del protocolo a ciertos ataques posibles (el ataque de repetición, el ataque de MIMT (*Man in the Middle*), ataque de suplantación, el ataque de fuga de secretos efímeros (ESL), ataque de privilegiado, preservación de las propiedades de anonimato e imposibilidad de rastreo, la captura física de IMD y los ataques en el servidor de la nube). También realizan una verificación de seguridad formal mediante un software de validación automatizada llamado “AVISPA”. Por último, llevan a cabo un análisis de rendimiento, además de una comparación con otros sistemas existentes y una simulación para medir el impacto de los parámetros de rendimiento. Tras todos estos análisis, concluyen que BAKMP-IoMT otorga una gestión de claves segura entre las diferentes entidades que se comunican y que además se comporta mejor en términos de seguridad y funcionalidad.

En [12] utilizan Blockchain para un marco de m-Health abordando los desafíos de seguridad, integridad y procedencia de los datos. Realizan una aplicación descentralizada de m-Health la cual monitorea los parámetros del paciente a través de sensores portátiles usando una cadena de bloques de Ethereum privada. Para evaluar el marco propuesto, utilizan señales reales recopiladas por sensores y comparan el rendimiento de la aplicación evaluando los tiempos de ahorro para los datos y los contrastan con un enfoque de datos centralizado clásico utilizando una base de datos MySQL relacional.

En [8] plantean la integración de Blockchain y la computación de borde, denominado Health-BlockEdge, con un enfoque particular en el impacto que tendría esto en la eficacia y eficiencia de los sistemas de monitoreo de salud remoto. Realizan una simulación de su propuesta considerando un caso de uso con y sin aplicar Blockchain y evaluaron los resultados de acuerdo con las métricas de desempeño definidas, las cuales eran: latencia, consumo de energía, costo de comunicación, costo computacional, número de operaciones ejecutadas y uso de la red. A partir de los resultados concluyeron que su propuesta mejora la protección de la privacidad de los datos y cumple con los requisitos de anonimato, también su concepto demostró viabilidad de uso para otorgar confianza descentralizada en tiempo real y control de la red, y la capacidad computacional en el entorno médico digital sin comprometer el rendimiento del sistema y eficiencia de recursos.

En [16] abordan los beneficios de implementar IoMT en el área de salud, así como las oportunidades de utilizar la tecnología Blockchain para la atención médica. También hacen una comparación entre la computación en la nube y Blockchain, y un análisis sobre la convergencia de estas dos tecnologías, BlockCloud. Por otra parte, analizan la arquitectura de Blockchain necesaria para su implementación en salud y su conexión con IA. Por último, tratan algunos aspectos sobre la seguridad y privacidad de los datos mediante Blockchain.

Por último, una presentación publicada por HL7 acerca del uso de Blockchain en salud muestra un esquema el que se analiza cuando realmente es necesario utilizar la cadena de bloques, a la vez que menciona algunas de sus características y plantea algunos casos de uso [22].

En Tabla 2 se presenta un resumen de los tipos de cadenas de bloques implementadas para cada artículo donde se observa una tendencia por el uso de cadenas de bloques de tipo consorcio o privadas, la utilización de contratos inteligentes para diferentes propósitos como la verificación de firmas y el almacenamiento de los datos sensibles fuera de ella.

TABLA II
Comparación entre las cadenas de Blockchain implementadas para cada artículo

Referencia	Tipo de Blockchain	Protocolo de consenso	Uso de contrato inteligente	Almacenamiento de los datos
Griggs [10]	Privada y dirigida por consorcio	PBFT	Sí, modular y personalizable	No se almacenan en la cadena, sólo el registro de las transacciones
Dwivedi [7]	Pública + Doble cifrado	-	Sí, para generar alertas de acuerdo con valores umbrales de las lecturas hechas por dispositivos ponibles	Utilizan la nube para almacenar los bloques de datos encriptados

Tripathi [18]	Cadena de dos niveles, una privada y otra pública	-	Sí	-
Meng [14]	Consorcio	-	Sí	-
Dai [19]	Consorcio, privada	-	Sí	
Garg [5]	Privada	-	-	Se almacenan en la nube para su posterior procesamiento
Taralunga [12]	Privada	Permite cualquier tipo de protocolo	Sí	Los datos sin procesar se almacenan como archivos JSON en IPFS
Ejaz [8]	Consorcio	-	-	-
Zhang [15]	-	-	Sí, para el almacenamiento ubicuo y registros de eventos de acceso a datos	Almacenan en la cadena, manteniendo fuera de ella los datos sensibles
Peterson [20]	Consenso	Prueba de interoperabilidad	Sí, para que el paciente de acceso a su registro sólo bajo ciertas condiciones	Las transacciones hacen referencia a los recursos FHIR, no al documento real.
1upHealth [21]	-	-	Sí, para almacenamiento y verificación	La cadena de bloques no almacena datos sensibles

Fuente: Elaboración propia.

4.3.1 LIMITACIONES

Tras la lectura de los artículos se observaron las siguientes limitaciones al momento de desarrollar un método para la implementación de Blockchain para la tecnología IoMT.

En [10] mencionan que las principales limitaciones con que se encontraron fueron las siguientes:

- La gestión de claves, ya que se podía volver un problema al momento de haber muchos dispositivos conectados transmitiendo sus transacciones a múltiples nodos y esperando su verificación.
- El retraso producido por los tiempos de verificación de los bloques.
- La sincronización de las transmisiones, ya que existe una diferencia entre el tiempo que toma el recopilar y agregar los datos y el tiempo que se demoran luego los datos en ser enviados, por lo que no aconsejan el uso de este sistema en caso de emergencias.
- El número de nodos mínimos necesarios para las firmas de validación y así mantener el algoritmo de consenso al tratarse de una cadena de bloques de tipo consorcio.
- También mencionan que, al momento de tratar de implementar la cadena de bloques enfocada en el paciente, se presentan problemas con el tamaño de los bloques, ya que estos están pensados para almacenar transacciones con declaraciones breves. Entonces el colocar registros sanitarios completos dentro de Blockchain aumentaría demasiado el tamaño de la cadena, lo cual requeriría un mayor almacenamiento por nodo.

En el contexto de IoMT, según [7] la implementación de la cadena de bloques conlleva algunos problemas, por lo que mencionan ciertos requisitos necesarios de considerar:

- **Descentralización**. Utilizar un sistema descentralizado garantiza la robustez y escalabilidad del sistema, además de eliminar los puntos de fallo único y los problemas de retraso de la información.

- **Autenticación de datos**. Es necesario un sistema de clave o firma para garantizar que los datos no se modifiquen o pierdan al momento del intercambio o transmisión de ellos.
- **Escalabilidad.** Los dispositivos IoMT tiene recursos limitados y su red también contiene muchos nodos, esto hace que Blockchain no se adapte bien a medida que estos aumentan, de modo que resolver el concepto de PoW requiere una gran potencia de cálculo, entonces eliminan este concepto y dividen la cadena de bloques en varios clusters.
- **Almacenamiento de datos**. Almacenar los big data de IoMT no sería práctico, entonces recomiendan utilizar servidores en la nube para almacenar bloques de datos encriptados.
- **Anonimato de los usuarios**. Debido a tratarse de datos sensibles, es importante que estos sean anónimos en la red.
- **Seguridad de los datos**. Es necesario considerar algún algoritmo cifrado o encriptación con tal de proteger los datos y evitar ataques informáticos en que los datos sean modificados o utilizados para un mal uso. En [7] utilizan un esquema de doble cifrado.

En [18] consideran que la aplicación de Blockchain en el dominio de la salud se está quedando atrás en comparación con otras áreas, y que esto se debe principalmente a la falta de expertos en Blockchain en el área de la salud. También identifican otros desafíos para la adopción de la cadena de bloques en salud, tales como:

- Falta de mecanismo estándar de recogida, intercambio e interoperabilidad de los datos.
- Si un paciente no está en condiciones de dar acceso a su información médica (por ejemplo, en casos de inconsciencia, la influencia de drogas o alcohol, entre otros motivos), entonces los contratos inteligentes no serían posibles.
- Problemas de migración de los datos desde el registro médico electrónico a Blockchain.
- Ausencia de políticas gubernamentales estándar y protocolos que definan reglas y regulaciones del uso adecuado de la tecnología Blockchain.

En [14] se centran en prevenir ataques internos en la cadena de bloques, y a pesar de tener resultados positivos también identifican ciertos desafíos que aún falta revolver, entre ellos:

- Limitaciones de la cadena de bloques, tales como la necesidad de una gran potencia de cálculo para el proceso de minería, privacidad de los datos, y posible retraso en la actualización de los bloques.
- Falta de expertos en TI para manejar las tareas de TI y proteger la seguridad de los datos.
- Sistema heredado y actualización tardía.
- Gestión de confianza centralizada hace vulnerable a ciberataques, por lo que recomiendan la implementación de una arquitectura distribuida para reducir este riesgo.
- Ataques externos.
- Aumento de la carga de trabajo.
- Rendimiento de IDS (*Instrusion Detection System*).

En [19] mencionan la baja escalabilidad como unas de las principales limitaciones de los sistemas actuales de Blockchain de tipo público, por esto recomiendan la adopción de cadena de bloques de tipo consorcio o privadas.

4.4 MÉTODOS DE IMPLEMENTACIÓN

En esta sección se analiza para cada documento encontrado qué indicadores de impacto se presentan con respecto a la pregunta de investigación de esta revisión sistemática, la cual busca la implementación de IoMT haciendo de uso de la tecnología blockchain para la seguridad y privacidad de los datos, y también el estándar FHIR para el intercambio de ellos.

TABLA III
Factor de impacto entregado por los documentos para la respuesta de la pregunta de investigación.

Referencia	Concepto	Impacto sobre la pregunta de investigación
Kim [9]	FHIR	Al tratarse de un estándar, FHIR permite que los datos sean verificables, permitiendo el intercambio de ellos entre los sistemas de información en salud.
Griggs [10]	Blockchain	El método de implementación de Blockchain propuesto fue realizado respetando los requisitos de HIPAA por lo que la preocupación acerca de la seguridad y privacidad de los datos estaría cubierto. Además, el sistema entregaría registros autentificados e inmutables. De esta forma Blockchain mejoraría la seguridad en los sistemas de monitorización remota de pacientes, además de permitir una mejor gestión de los datos y el uso de big data.
Peng, [11]	FHIR	Los autores mencionan que el método presentado tiene el potencial de apoyar la autogestión de la salud al integrar datos heterogéneos con distintos niveles de interoperabilidad.
Dwivedi, [7]	Blockchain	El método implementado y evaluado por los autores garantiza los requisitos de seguridad y privacidad pudiendo ser utilizado por cualquier sistema de monitorización remota basado en IoT.
Tripathi [18]	Blockchain	Si bien los autores entregan un análisis más conceptual, el método propuesto apunta a preservar seguridad y privacidad de los datos.
Meng, [14]	Blockchain	Este artículo plantea un enfoque interesante, ya que es el único que considera el uso de Blockchain para proteger a los MSN de los posibles ataques internos de un sistema IoMT, que según los autores es una de las principales amenazas.
Dai, [19]	Blockchain	Se observan parte de las múltiples aplicaciones que tiene IoMT y como Blockchain ayudaría a preservar la trazabilidad, la seguridad y la privacidad de los datos.
Garg [5]	Blockchain	El protocolo de gestión de claves basado en Blockchain para dispositivos IoMT garantiza la autenticación segura y legítima entre las entidades que se comunican, protegiendo así los datos sanitarios almacenados.
Taralunga, [12]	Blockchain	Utilizan Blockchain privado para solucionar los problemas de seguridad, integridad y procedencia de los datos.
Ejaz, [8]	Blockchain	Aquí el uso de Blockchain es combinado con la computación de borde y mencionan que este enfoque mejora la protección de la privacidad de los datos al limitar la propagación de datos sensibles en las redes locales y de borde en vez de enviarlos a la nube.
Zhang [15]	FHIR, Blockchain	La implementación de FHIRChain tendría la capacidad de otorgar almacenamiento descentralizado y sin confianza para la metainformación y los registros de auditoría. También facilita el intercambio de datos, manteniendo la propiedad de ellos. Además, la criptografía de clave pública utilizada permite administrar fácilmente la identidad digital en el intercambio de datos. De esta forma FHIRChain,

		fomentaría el intercambio efectivo de datos de salud manteniendo la seguridad de estos.
Mavrogiorgou [1]	FHIR	Aquí el impacto estaría en la capacidad de traducción de los datos obtenidos de los dispositivos IoMT con velocidades y rendimiento aceptable según las necesidades computacionales de cada escenario médico asignado por los autores.
Aileni [16]	Blockchain	El impacto está en la importancia de las aplicaciones de IoMT y las oportunidades que ofrece su combinación con Blockchain, entre ellas, la integridad y confiabilidad de la información y el acceso distribuido.
Peterson [20]	Blockchain, FHIR	La API implementada tiene características para rastrear la procedencia de los datos y asegurar su integridad, pudiendo también verificar la inmutabilidad de los datos.
1upHealth [21]	Blockchain, FHIR	Este documento muestra los primeros intentos para el intercambio efectivo de datos, teniendo como prioridad la seguridad de estos.

Fuente: Elaboración propia.

4.5 IMPLEMENTACIÓN DE ESTÁNDAR HL7 FHIR PARA IoMT

Al momento de abordar los temas sobre cómo realizar la recogida de datos, el intercambio la información, la difusión de datos a otras aplicaciones o bien el procesamiento de datos y extracción de información y conocimientos, dentro de la literatura revisada mencionan y coinciden en la importancia de un formato estándar en la recogida de datos para así lograr un mayor grado de interoperabilidad entre los sistemas de información y sus procesos. Por esto, el uso de HL7 FHIR es preferente al tratarse de un estándar internacional de datos sanitarios.

En [9] plantean una plataforma de recogida de datos, donde un dispositivo IoT se conecta a un PC o smartphone, el cual funciona como un PHR local (*Personal Health Record*), donde se generan los datos en formato FHIR, y se transmiten al servidor de datos sanitarios (actúa como un repositorio remoto de PHR), aquí los datos se pueden almacenar y consultar gracias a las funciones de API RESTful. Luego los datos se transfieren al servidor de datos públicos previa anonimización, en este servidor los datos son convertidos a formato FHIR y dispuestos al público.

En [11] proponen un método que sigue el camino de FHIR para aplicar tecnologías de la web semántica y el modelo de recursos REST para integrar los datos de salud y del entorno doméstico de los servicios construidos heterogéneamente como recursos asociados. El objetivo es vincular semánticamente los servicios de salud y los dispositivos WoT (*Web of Things*) que adoptaron FHIR, descritos como ontologías formales, implementados por APIs web RESTful o publicados como Linked Data (servicios con diferentes niveles de interoperabilidad). Estos datos heterogéneos son modelados como recursos de información conceptual utilizando la ontología *Linked Health Resources* (LHR). Establecen que para lograr una integración interoperable satisfactoria es necesario que los servicios involucrados en salud implementen estándares de interoperabilidad como HL7 FHIR y los dispositivos WoT implementen ontología de descripción como SSN (*Semantic Sensor Network*) y SOSA (*Sensor, Observation, Sample and Actuator*).

En [4] presentan una plataforma para IoMT la cual integra múltiples protocolos de comunicación y entrega funcionalidades para el almacenamiento de datos y la aplicación de técnicas OLAP (*online analytical processing*), así como también herramientas para la minería de datos a través de Hadoop. Esta se basa en una extensión semántica de OpenEHR para el dominio IoMT, siguiendo una

arquitectura de comunicación OneM2M que integra los dispositivos IoMT a una HCE basada en OpenEHR. En el artículo describen todo acerca de la arquitectura de la plataforma propuesta y su implementación. Para su evaluación, realizaron pruebas de rendimiento basadas en métricas, así como el diseño de un caso de uso para la prueba de concepto. Estas pruebas dieron buenos resultados y validaron la plataforma en los escenarios considerados. Afirman que esta plataforma garantiza la interoperabilidad desde la recogida hasta la publicación de los datos.

En [1] proponen una plataforma de extremo a extremo en que los dispositivos de IoMT para diferentes escenarios de aplicaciones que se conectan por WiFi mediante el mecanismo de adquisición de datos propuesto, donde se adquieren los datos de los dispositivos IoMT, así como sus especificaciones de red, para luego ser segmentados en diferentes cortes de red 5G a través del mecanismo de *Slicing Management*, atendiendo a los requerimientos de computación de los diferentes escenarios, además de hacer que los datos sean interoperables mediante su traducción al estándar HL7 FHIR.

4.5.1 LIMITACIONES DE IMPLEMENTACIÓN

Tras la lectura de los documentos y en busca de limitaciones existentes para la implementación de FHIR para el intercambio de información se halló lo siguiente:

Con respecto a la implementación del estándar HL7 FHIR, en [9] comentan que si bien la especificación básica de FHIR describe un grupo de recursos, marcos y API utilizadas en diferentes contextos en la asistencia sanitaria, existe una alta variabilidad entre jurisdicciones y en el ecosistema sanitario en lo que se refiere a las prácticas, los requisitos, la normativa, la educación y las acciones que son viables y útiles, por lo que es necesaria una mayor adaptación a contextos particulares de uso.

Otra limitación encontrada fue el hecho de que la implementación de FHIR puede no ser compatible con sistemas heredados que utilicen otros estándares de mensajería, como lo son los estándares HL7 v2 [15].

4.6 IMPLEMENTACIÓN DE BLOCKCHAIN Y ESTÁNDAR HL7 FHIR PARA IoMT

La pregunta de investigación se enfoca en encontrar evidencias sobre la implementación de estas dos tecnologías en conjunto para el desarrollo de aplicaciones IoMT considerando las características acerca de la privacidad, la seguridad y la interoperabilidad de los datos como los requisitos más relevantes. Sin embargo, dentro de la búsqueda de literatura no se hallaron artículos que incluyeran ambas tecnologías. Por esta razón se recurrió a la búsqueda de otros documentos técnicos para complementar la información y contribuir a una respuesta más apropiada de la pregunta objetivo.

A partir de una referencia utilizada en [15], se halló que para el año 2016, los autores de [20] propusieron un enfoque para el intercambio de datos de forma segura y eficaz mediante el uso de Blockchain basado en contratos inteligentes, donde las transacciones hacen referencia a los recursos FHIR y reemplazaron la prueba de trabajo por una prueba de interoperabilidad, la cual verifica que los mensajes ingresados sean interoperables respecto a las restricciones estructurales y semánticas impuestas por perfiles FHIR.

Por otra parte, los líderes en la implementación de FHIR, 1upHealth implementaron una plataforma API denominada "*FHIR Provenance + Blockchain*" en la que al momento de recopilar o ingresar los datos provenientes de algún sistema de salud conectado, se crea un recurso de procedencia FHIR y

simultáneamente se almacena un hash del recurso FHIR en la cadena de bloques de 1upHealth, la cual es ejecutada en una cadena lateral basada en Ethereum. Gracias a esta implementación, en el 2018 obtuvieron el primer lugar en el desafío de Procedencia de los Datos de Salud de la ONC [23]. Como trabajo a futuro, señalan la necesidad de avanzar en el cifrado cuántico para poder almacenar los datos cifrados de los pacientes en un servicio descentralizado como IPFS, sin poner en riesgo la seguridad de ellos [21].

En [15] presentan las consideraciones arquitectónicas que se deberían tener para la implementación de sistemas de intercambio de datos clínicos seguros y escalables basados en Blockchain, de acuerdo a los requisitos técnicos definidos por la ONC (Oficina del Coordinador Nacional de Tecnología de la Información en Salud). Además, presentan una arquitectura denominada FHIRChain, basada en Blockchain, y que también encapsula el estándar HL7 FHIR para el intercambio de datos. Para la demostración de la arquitectura FHIRChain implementan una aplicación descentralizada (DApp), enfocada en el cuidado del cáncer, la cual permite compartir información específica y estructurada, aumentando de esta forma la legibilidad de los datos y la flexibilidad de las opciones para compartir.

4.7 BRECHAS PARA IMPLEMENTAR IoMT

Tras la revisión de literatura, se encontraron las siguientes brechas o limitaciones al momento de implementar IoMT [4], [5], [9], [10], [12], [15], [18], [19].

- Ausencia de interoperabilidad entre los distintos sectores de IoMT debido a la heterogeneidad de los datos, con diferentes formatos y estándares que imposibilitan o dificultan la integración de estos.
- Necesidad de un sistema o método de anonimización para preservar la privacidad de los pacientes.
- Fallas del sistema
- Vulnerabilidad de la privacidad y seguridad de los dispositivos y sistemas de IoMT, siendo susceptibles a ataques de virus y delitos informáticos.
- Uso de unidad de monitoreo centralizada, lo que implica una alta probabilidad de pérdida o corrupción de los datos.
- Las prestaciones de los distintos protocolos de comunicación implementados en IoT/IoMT dependen de las funcionalidades que ofrecen, ya que se centran en enfermedades específicas, haciendo que uno sea más adecuado que otro dependiendo del contexto. Sin embargo, una plataforma IoMT debería ser adaptable para el uso de cualquier protocolo ya existente.
- La falta de propuestas para la integración del HCE con las plataformas de IoMT, hace que el HCE sea gestionado con registros distribuidos proporcionados por múltiples fuentes.
- El volumen y la complejidad de los datos recopilados en las soluciones IoMT dificultan su interpretación por parte de los médicos, lo que a su vez dificulta el trabajo de Big Data.
- Desafíos referentes a factores humanos, como el nivel de conocimiento técnico de una persona y la adaptabilidad para aprovechar las ventajas que ofrece la tecnología IoT, como también, la necesidad de considerar las capacidades de los pacientes para la adopción de dispositivos portátiles de IoMT, en lo que respecta al conocimiento del sistema y su capacidad para utilizar la tecnología eficazmente.
- Almacenamiento de los ensayos clínicos de forma insegura y sin cuidado de preservar la privacidad de estos, por lo que no pueden ser utilizados para investigaciones o estudios.
- Falta de relaciones de confianza entre las distintas instituciones sanitarias.

4.8 IMPACTO EN LA SOCIEDAD DE IMPLEMENTAR IoMT

La implementación de IoMT presentaría beneficios importantes para la calidad de atención de los pacientes, así como para las instituciones de salud. A continuación, algunas de las ventajas más destacadas por los autores de los artículos con respecto al desarrollo de IoMT.

En [9] mencionan que a través de la aplicación de la plataforma implementada se tendría la posibilidad de ayudar a los pacientes con Parkinson pudiendo otorgar servicios personalizados de acuerdo a los resultados obtenidos por la plataforma, así como ayudar a ajustar el suministro de medicamentos, mejorar los métodos de tratamiento y la comprensión del curso del tratamiento según datos sanitarios objetivos.

En [10] destacan una ventaja de su sistema implementando, y es que el uso de Blockchain en su sistema proporciona registros autenticados e inmutables de un paciente que ayudarían a resolver disputas o investigar. También el sistema al estar enfocado en el paciente permite que múltiples dispositivos IoMT se vinculen al paciente.

El uso de dispositivos IoMT para la monitorización remota de pacientes de acuerdo a [7] tendría varias ventajas, entre ellas: permite a los médicos tratar a más pacientes, comodidad para los pacientes, conexión de los pacientes con el proveedor de atención médica en cualquier momento, reducción de los costos médicos y mejora en la calidad de atención.

5. DISCUSIÓN

En base a los resultados obtenidos se puede apreciar que existe un gran interés en la aplicación de Blockchain en el área de salud, siendo los esfuerzos de investigación mayormente enfocados en contribuir con soluciones para la seguridad, la privacidad, e inmutabilidad de los datos. Para el logro de este objetivo en los artículos se observó principalmente el uso de contratos inteligentes, cadenas de tipo consorcio y privadas, el cifrado de las transacciones y el no almacenamiento de datos sensibles dentro de los bloques, sino que sólo el registro de las transacciones. En gran parte de los artículos se menciona adecuado el uso de Blockchain para las aplicaciones de atención médica, ya que el uso de criptografía permitiría un intercambio seguro entre las distintas instituciones de salud. Sin embargo, es de vital importancia el desarrollo de protocolos y estándares sobre cómo implementar Blockchain en salud para su correcta aplicación, así como llegar a acuerdos acerca de la infraestructura y conexiones más adecuadas.

Por otro lado, para lograr una salud conectada, lograr la interoperabilidad de los datos es uno de los requisitos más importantes dentro un sistema de información de salud, por esta razón es necesario aumentar la investigación que cubra la adopción del estándar FHIR para el formato de los datos en cualquier sistema de salud y así lograr una mejor gestión e intercambio de la información.

El rompimiento de las brechas encontradas en la implementación de las tecnologías tratadas sería un aporte positivo en la gestión de la salud y favorece de manera considerable la calidad en la atención médica, mejorando así también la calidad de vida de las personas en general, pudiendo permitirles un mayor control sobre su salud, en especial a personas postradas en su domicilio o que por alguna enfermedad no pueden movilizarse fácilmente hasta un establecimiento de salud. Al ver esto desde

una perspectiva nacional, y pensando en las aplicaciones de monitorización remota o atención domiciliaria, el implementar estas tecnologías IoMT a corto plazo podría ser algo ambicioso, ya que el coste de implementación de estas podría ser una limitación a causa de la deuda hospitalaria existente en la salud pública de Chile [24]. En una primera instancia, se debería avanzar de manera paulatina y comenzar a implementarlo en el sector privado, donde existen mayor cantidad de recursos.

Por otra parte, al hacer un análisis interno de este trabajo se encontró que una de las limitaciones que se presentaron fue la poca cantidad de artículos enfocados en el uso de Blockchain y el estándar FHIR para la implementación de las tecnologías IoMT, generando la necesidad de buscar artículos en otras fuentes y de esta manera, encontrar la información suficiente para contestar a la pregunta de investigación, en consecuencia, una de las fortalezas de este trabajo, es que aborda terreno casi inexplorado en cuanto al uso conjunto de estas tres tecnologías emergentes, un enfoque que aún es necesario profundizar.

Por último, durante la búsqueda de artículos de otras fuentes, se halló un artículo que trataba sobre el diseño de un sistema de tecnología mayor distribuido para el intercambio de datos salud interoperable, IOTA que es distinto de Blockchain motivo por el cual no se incluyó en la revisión sistemática, pero que podría también considerarse en otras investigaciones [25].

6. CONCLUSIÓN

El trabajo de revisar la aplicación de las tecnologías tratadas en esta búsqueda de literatura permitió identificar la tendencia de los trabajos futuros en salud para lograr una gestión e intercambio de los datos sanitarios de forma segura y efectiva.

Durante la búsqueda sistemática, en lo que se refiere al desarrollo de IoMT se observó un mayor trabajo en la creación de aplicaciones IoMT para distintas finalidades, pero en realidad muy pocos artículos considerando soluciones para los aspectos de seguridad y privacidad de estas, así como la posibilidad de intercambio de los datos manejados por estas aplicaciones. Los pocos artículos que tenían en cuenta estos aspectos estaban enfocados en un tipo particular de dispositivo IoMT, por lo que no se sabe si los métodos implementados son aplicables para toda la gama de dispositivos IoMT. Asimismo, no se encontró un acuerdo en el método de implementación para Blockchain, aunque la tendencia es a una cadena descentralizada y el uso de contratos inteligentes.

En cuanto a la pregunta objetivo de esta revisión, la búsqueda de documentos científicos no arrojó resultados para la combinación de las tecnologías Blockchain y el estándar FHIR para el desarrollo de aplicaciones IoMT, pero sí al buscar documentos técnicos se identificaron dos artículos que principalmente planteaban los requisitos o consideraciones para la implementación y combinación de estas tecnologías. Además, también se obtuvo un resultado que llevó a cabo esta implementación, la cual, aunque funciona, aún se encuentra en proceso de desarrollo para poder hacerla accesible a una mayor cantidad de sistemas de salud.

Entre las principales brechas para la implementación de aplicaciones IoMT, la mayoría de los autores coincide en que son los problemas de seguridad, privacidad, integridad e interoperabilidad de los datos, por lo que la integración con la cadena de bloques y el estándar FHIR tendría el potencial de mejorar la implementación de IoMT y transformar el área de salud a un sistema más conectado, seguro y que cuida la información sensible de los usuarios de manera ética y sistemática.

Por esta razón, de acuerdo con los resultados obtenidos, se observa que la implementación y combinación de las tecnologías de Blockchain, IoMT y el estándar de HL7 FHIR puede ser posible, pero su desarrollo aún se encuentra en una etapa inicial debido a lo emergente de ellas. En consecuencia, aún falta la realización de más estudios e investigaciones para profundizar en el tema y así obtener resultados más concretos acerca de cómo implementar adecuadamente estas tecnologías y en lo posible desarrollar protocolos o estándares que lo regularicen.

7. REFERENCIAS

[1] A. Mavrogiorgou, K. Athanasios, M. Touloupou, E. Kapassa, y D. Kyriazis, "Internet of Medical Things (IoMT): Acquiring and Transforming Data into HL7 FHIR through 5G Network Slicing", *Emerg. Sci. J.*, vol. 3, nº 2, pp. 64–77, 2019, doi: 10.28991/esj-2019-01170.

[2] Servicio Nacional del Adulto Mayor, "Guía de Orientaciones Técnicas, Programa Cuidados Domiciliarios", 2017. [En línea]. Disponible en: http://www.senama.gob.cl/storage/docs/Guia_de_Orientaciones_Tecnicas_PCD_VERSION_RESOLUCION_09_08_2017_-_copia.pdf.

[3] Ministerio Secretaría General de la Presidencia, *Ley 19628 Sobre la protección de la vida privada*. Chile: Biblioteca del Congreso Nacional de Chile, 2020, p. 2.

[4] J. N. S. Rubí y P. R. L. Gondim, "IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR", *Sensors*, vol. 19, nº 19, p. 4283, oct. 2019, doi: 10.3390/s19194283.

[5] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, y Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment", *IEEE Access*, vol. 8, pp. 95956–95977, 2020, doi: 10.1109/ACCESS.2020.2995917.

[6] L. Sun, X. Jiang, H. Ren, y Y. Guo, "Edge-Cloud Computing and Artificial Intelligence in Internet of Medical Things: Architecture, Technology and Application", *IEEE Access*, vol. 8, pp. 101079–101092, 2020, doi: 10.1109/ACCESS.2020.2997831.

[7] A. D. Dwivedi, G. Srivastava, S. Dhar, y R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT.", *Sensors (Basel).*, vol. 19, nº 2, ene. 2019, doi: 10.3390/s19020326.

[8] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, y E. Harjula, "Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications", *Sensors*, vol. 21, nº 7, p. 2502, abr. 2021, doi: 10.3390/s21072502.

[9] D.-Y. Kim, S.-H. Hwang, M.-G. Kim, J.-H. Song, S.-W. Lee, y I. K. Kim, "Development of Parkinson Patient Generated Data Collection Platform Using FHIR and IoT Devices.", *Stud. Health Technol. Inform.*, vol. 245, pp. 141–145, 2017, [En línea]. Disponible en: http://www.ncbi.nlm.nih.gov/pubmed/29295069.

[10] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, y T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", *J. Med. Syst.*, vol. 42, nº 7, p. 130, jul. 2018, doi: 10.1007/s10916-018-0982-x.

[11] C. Peng y P. Goswami, "Meaningful Integration of Data from Heterogeneous Health Services and Home Environment Based on Ontology.", *Sensors (Basel).*, vol. 19, nº 8, abr. 2019, doi: 10.3390/s19081747.

[12] D. D. Taralunga y B. C. Florea, “A Blockchain-Enabled Framework for mHealth Systems”, *Sensors*, vol. 21, nº 8, p. 2828, abr. 2021, doi: 10.3390/s21082828.

[13] D. Mendes, I. P. Rodrigues, C. Fonseca, M. J. Lopes, J. M. García-Alonso, y J. Berrocal, “Anonymized Distributed PHR Using Blockchain for Openness and Non-Repudiation Guarantee.”, *Stud. Health Technol. Inform.*, vol. 255, pp. 170–174, 2018, [En línea]. Disponible en: http://www.ncbi.nlm.nih.gov/pubmed/30306930.

[14] W. Meng, W. Li, y L. Zhu, “Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks”, *IEEE Trans. Eng. Manag.*, vol. 67, nº 4, pp. 1377–1386, 2020, doi: 10.1109/TEM.2019.2921736.

[15] P. Zhang, J. White, D. Schmidt, G. Lenz, y S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data”, *Comput. ans Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018, doi: https://doi.org/10.1016/j.csbj.2018.07.004.

[16] R. M. Aileni y G. Suciu, “IoMT: A Blockchain Perspective”, en *Studies un Biga Data 71*, Bucharest: Springer, 2020, pp. 199–215.

[17] HL7, “FHIR Overview - Architects”, 2019. https://www.hl7.org/fhir/overview-arch.html.

[18] G. Tripathi, M. A. Ahad, y S. Paiva, “S2HS- A blockchain based approach for smart healthcare system.”, *Healthc. (Amsterdam, Netherlands)*, vol. 8, nº 1, p. 100391, mar. 2020, doi: 10.1016/j.hjdsi.2019.100391.

[19] H.-N. Dai, M. Imran, y N. Haider, “Blockchain-Enabled Internet of Medical Things to Combat COVID-19”, *IEEE Internet Things Mag.*, vol. 3, nº 3, pp. 52–57, 2020, doi: 10.1109/IOTM.0001.2000087.

[20] K. Peterson, R. Deeduvanu, P. Kanjamala, y K. Mayo, “A Blockchain-Based Approach to Health Information Exchange Networks”, *Comput. Sci.*, 2016, [En línea]. Disponible en: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf.

[21] 1upHealth, “Blockchain FHIR Provenance”, *1upHealth Docs*, 2021. https://1up.health/docs/api/blockchain-fhir-provenance.

[22] E. Kramer, “Blockchain & Healthcare Standards”. HL7, Amsterdam, 2018, [En línea]. Disponible en: https://www.hl7.org/documentcenter/public/calendarofevents/himss/2018/Blockchain and Healthcare Standards.pdf.

[23] The Office of the National Coordinator for Health Information Technology, “Provenance Challenge”, *Capital Consulting Corporation Innovation Center*, 2018. https://www.cccinnovationcenter.com/challenges/provenance-challenge/.

[24] Subsecretaria de redes asistenciales, “Deuda Hospitalaria”. [En línea]. Disponible en: https://www.senado.cl/site/presupuesto/2020/cumplimiento/Glosas 2020/16 Salud/713 Deuda Hospitalaria 2020.pdf.

[25] D. Hawig, C. Zhou, S. Fuhrhop, F. Andre, y N. Ramachandran, “Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation-Compliant Health Data Exchange: A Use Case in Blood Glucose Data”, *J. Med. Internet Res.*, vol. 21, nº 6, 2019, doi: 10.2196/13665.