

Artículo original

Informe Sanitario Res. Enero de 2020;26(1):3-12.
<https://doi.org/10.4258/hir.2020.26.1.3> pISSN
 2093-3681 • eISSN 2093-369X

HIR

Healthcare Informatics Research

Aplicación de Blockchain para mantener registros de pacientes en registros médicos electrónicos para mejorar la privacidad, la escalabilidad y la disponibilidad

Dara Tith, Joong-Sun Lee, Hiroyuki Suzuki, WMAB Wijesundara, Naoko Taira, Takashi Obi, Nagaaki Ohyama

Instituto de Investigación Innovadora, Instituto de Tecnología de Tokio, Yokohama, Japón

Objetivos: Los sistemas de Historia Clínica Electrónica (EHR) se utilizan cada vez más como un método eficaz para compartir los registros de los pacientes entre diferentes hospitales. Sin embargo, sigue siendo un desafío acceder a datos dispersos de pacientes a través de múltiples EHR. Nuestro objetivo es construir un sistema para acceder fácilmente a los registros de pacientes entre los EHR sin depender de un sistema de supervisión centralizado. **Métodos:** Aplicamos blockchain de consorcio para componer un sistema distribuido utilizando Hyperledger Fabric incorporando EHR existentes. Los nodos pares mantienen el mismo libro de contabilidad en el que se escribe la dirección del registro de un paciente en un EHR. Los pacientes individuales se identifican mediante certificados únicos emitidos por autoridades de certificación locales que colaboran entre sí en un canal de la red. Para proteger la privacidad de un paciente, utilizamos un esquema de cifrado de proxy cuando se transfieren los datos. Diseñamos e implementamos varios códigos de cadena para manejar la lógica empresarial acordada por las organizaciones miembros de la red. **Resultados:** Desarrollamos un sistema prototípico para implementar nuestro concepto y probamos su rendimiento, incluida la lógica del código de cadena. Los resultados demostraron que los médicos pueden utilizar nuestro sistema para encontrar los registros de los pacientes y verificar el consentimiento del paciente al acceder a los datos. Los pacientes también pueden recibir sin problemas sus registros anteriores de otros hospitales. El registro de acceso se almacena de forma transparente e inmutable en el libro de contabilidad que se utiliza con fines de auditoría. **Conclusiones:** Nuestro sistema es factible y flexible con escalabilidad y disponibilidad para adaptarse a los EHR existentes para fortalecer la seguridad y la privacidad en la gestión de registros de pacientes. Se espera que nuestra investigación proporcione un método eficaz para integrar registros de pacientes dispersos entre instituciones médicas.

Palabras clave: Intercambios de información de salud, registros médicos electrónicos, privacidad de datos de pacientes, seguridad informática, descentralización

Enviado: 13 de septiembre de 2019

Revisado: 8 de noviembre de 2019

Aceptado: 29 de noviembre de 2019

Autor correspondiente

Joong Sun Lee
 R2-60 Instituto de Tecnología de Tokio, 4259 Nagatsuta, Midori-ku,
 Yokohama, Kanagawa 226-8503, Japón. Tel: +81-0459245482, Correo
 electrónico: j-lee@isl.titech.ac.jp (<https://orcid.org/0000-0002-6976-6472>)

Este es un artículo de acceso abierto distribuido bajo los términos de la licencia no comercial de atribución Creative Commons (<http://creativecommons.org/licenses/bync/4.0/>) que permite el uso, la distribución y la reproducción sin restricciones y sin fines comerciales en cualquier medio, siempre que se cite debidamente la obra original.

© 2020 Sociedad Coreana de Informática Médica

I. Introducción

Los sistemas de Historia Clínica Electrónica (EHR) [1] se han utilizado cada vez más como un método eficaz para compartir los registros de los pacientes entre diferentes hospitales. Sin embargo, sigue siendo un desafío acceder a datos dispersos de pacientes a través de múltiples EHR porque los EHR existentes están limitados regionalmente o pertenecen a hospitales afiliados. Según el informe publicado por la Oficina del Coordinador Nacional de Tecnología de la Información en Salud (ONC) [2], la principal barrera para acceder a los registros de los pacientes radica en la dificultad para encontrar las direcciones de los proveedores. Hasta ahora, ha habido varios proyectos para superar estos problemas; sin embargo, las soluciones que han producido son difíciles y

implicaría rediseñar o mejorar los sistemas EHR existentes, lo que requeriría gastos sustanciales. Entre ellos, uno de los programas más activos es el dirigido por CommonWell Health Alliance [3] en Estados Unidos, una asociación sin fines de lucro. Apoyan a los EHR, los proveedores de atención y los proveedores de tecnología de la información sanitaria (HIT) para conectarse a su red de interoperabilidad a nivel nacional a través de intermediarios y plataformas de integración certificadas. Utilizan un sistema centralizado que permite a los pacientes y médicos buscar registros médicos dispersos de un paciente [4]. Una arquitectura tan centralizada tiene algunos inconvenientes: puede enfrentar el riesgo de un punto único de falla y un cuello de botella en el flujo de datos cuando el sistema crece.

En un sistema EHR, cuando se accede a los registros de pacientes por algún motivo, el historial de todos esos eventos debe registrarse en un archivo de registro para una auditoría posterior de los históricos de acceso. El archivo de registro se utiliza para reconstruir el estado anterior de los registros médicos y puede representarse como un documento legal [5-7]. Por lo tanto, debemos proteger firmemente el archivo de registro del acceso ilegal y hacerlo inmutable si es posible.

En este artículo, proponemos un sistema descentralizado para abordar los problemas al compartir registros de pacientes entre los EHR sin depender de un sistema centralizado de alto nivel. Nuestro sistema tiene tres características principales: (1) un directorio confiable de datos de pacientes en

EHR que garantiza el acceso así como la integridad de los datos en sí, (2) seguridad reforzada al tratar con datos de pacientes mediante la utilización de un esquema de cifrado particular y proporcionando un registro de auditoría transparente e innegable basado en un registro de acceso inmutable, y (3) proporcionando escalabilidad para cubrir múltiples EHR existentes de hospitales regionales o centrales con la menor modificación y disponibilidad del sistema sin depender de un sistema de supervisión centralizado.

Diseñamos el sistema siguiendo la salvaguardia técnica de la Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA) [8] e ISO/TS 18308 [5] para la interoperabilidad, integridad de los datos, auditabilidad y disponibilidad del sistema. Para lograr nuestros objetivos, adoptamos la tecnología blockchain, especialmente el tipo de consorcio autorizado [9], utilizando la plataforma Hyperledger Fabric (HLF). Varios hospitales se reúnen para formar un consorcio que tiene una red privada de igual a igual, y el permiso para unirse se determina en función del consenso entre los miembros.

HLF es una plataforma de código abierto que tiene muchos componentes esenciales disponibles en algunos lenguajes de programación. Además, proporciona el protocolo de consenso bizantino tolerante a fallos [10] para ordenar transacciones en un bloque. Además, permite un rendimiento de extremo a extremo [11] de más de 3500 transacciones por segundo. Es un proyecto [12] organizado por la

Tabla 1. Componentes de Hyperledger Fabric

Descripción	
Libro mayor	Consiste en una cadena de bloques y una base de datos estatal [12] (también conocida como estado mundial). El primero es un registro de transacciones, mientras que este último contiene los valores actuales de los estados del libro mayor. Gracias a la base de datos de estado, el programa obtiene valores fácilmente sin tener que recorrer todo el registro de transacciones. Las transacciones [13-15] se recopilan para formar un bloque que se agrega secuencialmente al último bloque de la cadena de bloques, que es inmutable una vez realizado.
Roles del usuario	Hay tres tipos principales de roles de usuario: cliente, par (que respalda y promete uno) y ordenante. Un compañero es un nodo de red, y los pares que respaldan, simplemente llamados patrocinadores, realizan el respaldo simulando la propuesta de transacción de un cliente. La propuesta es una transacción tentativa antes de ser aceptada en un nuevo bloque del libro mayor. Un ordenante ejecuta un servicio de pedidos para crear un nuevo bloque con transacciones y luego transmite el bloque a todos los pares. Un par comprometido, también llamado confirmador, actualiza el libro mayor agregándole el nuevo bloque y revisando la base de datos de estado con los conjuntos de escritura de transacciones válidas.
Código de cadena	Es un programa de aplicación ejecutado por pares para facilitar, verificar o hacer cumplir la negociación y el acuerdo entre usuarios. Un código de cadena también se conoce como contrato inteligente en otras plataformas blockchain como Ethereum. Un código de cadena [16] tiene muchas funciones de programación y, por lo general, lee y actualiza el estado del libro mayor con toda la lógica empresarial contenida dentro de las funciones.
Servicio de membresía proveedor (MSP)	MSP [17] tiene como objetivo abstraer todos los mecanismos y protocolos criptográficos detrás de la emisión y validación de certificados, certificados y autenticación de usuario. Hay dos tipos de MSP, canal y local. Un MSP de canal proporciona un método para validar certificados de inscripción (ECerts) entre diferentes organizaciones del canal, mientras que un MSP local ofrece un método para verificar la identidad de un usuario en una organización. Por lo tanto, cada organización tiene su MSP local con un ID de MSP único y emite ECerts, certificados X.509, a todos los participantes locales con ID de inscripción (eID) a través de su autoridad de certificación (CA).

Linux Foundation, y las contribuciones al proyecto las realizan Digital Asset e IBM.

II. Métodos

1. Tejido Hyperledger

En HLF, hay varios componentes clave (Tabla 1) que desempeñan papeles fundamentales en el sistema. Además, proporciona tres fases de consenso (Tabla 2) para validar las transacciones antes de cargarlas en el libro mayor. HLF proporciona una variedad de códigos de cadena designados especiales llamados códigos de cadena del sistema para realizar ciertas tareas privilegiadas. Ejemplos de códigos de cadena del sistema son códigos de cadena del sistema de configuración, ciclo de vida, consulta, endoso y validador. En nuestro estudio, diseñamos varios códigos de cadena de requisitos previos y los implementamos en nuestro sistema prototípico.

2. Diseño Conceptual del Sistema

Construimos una subred privada de una red HLF donde se comparte el mismo libro de contabilidad entre los miembros del hospital (Figura 1), lo que se denomina canal. Las organizaciones o departamentos dentro de ellas pueden constituir canales independientes con libros de contabilidad relevantes según sus necesidades. En la práctica, los datos médicos suelen ser demasiado grandes para manejarlos directamente en un libro mayor; por lo tanto, los datos se guardan en un EHR y solo se registra la dirección en el libro mayor. Este tipo de almacenamiento se denomina dentro o fuera de la cadena según si los datos están en un libro mayor o no [15]. Un libro mayor también contiene los valores hash de los datos. Esto garantiza la integridad de los datos porque una vez que un dato se escribe en un libro mayor, se vuelve inmutable y esto permite al usuario verificar si los datos han sido alterados o no.

En nuestro sistema, asumimos que un cliente de HLF (Tabla 1) es un médico, enfermero o empleado que ayuda a los pacientes a cargar o compartir sus registros médicos. Los clientes de instituciones médicas realizan varios tipos de transacciones y las almacenan en un libro mayor. El libro de contabilidad consta de metadatos de pacientes, incluidos datos demográficos,

y estos datos se utilizan para solicitudes de recuperación para encontrar transacciones relacionadas con un paciente específico durante un período específico de marcas de tiempo de bloques en el libro mayor. Por lo tanto, el libro de contabilidad funciona como un registro de identificaciones de pacientes para que los médicos busquen los registros de sus pacientes almacenados en otros EHR. Además, cada transacción contiene los metadatos de la solicitud del cliente, los resultados de la ejecución del código de cadena y los metadatos de los registros médicos, como la identificación del hospital, el hash de los registros médicos almacenados en un EHR, etc. En consecuencia, estos datos se utilizarán con fines de auditoría.

Para un paciente individual, la identificación de inscripción (eID) emitida por un proveedor de servicios de membresía (MSP) se utiliza como identificación del paciente del canal en el sistema. Cada transacción en el libro mayor contiene un eID, que se codifica después de concatenarse con datos aleatorios llamados salt [19] en el formato que se muestra a continuación:

$\$n \$sal \$hash (sal + eID)$.

Este formato es casi el mismo que el sistema Linux almacena las contraseñas hash de sus usuarios con sales. Aquí, “\$” se utiliza como delimitador entre campos vecinos; “n” representa

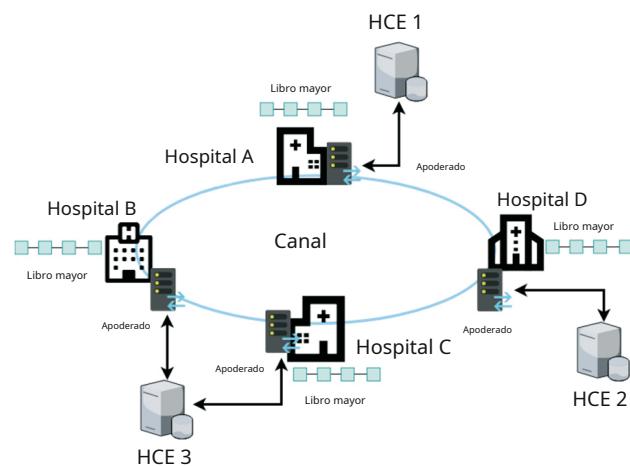


Figura 1. Canal de red entre instituciones médicas con el mismo libro mayor. HCE: Historia Clínica Electrónica.

Tabla 2. Tres fases de consenso para validar transacciones en Hyperledger Fabric

		Descripción
Aprobación		Los patrocinadores simulan la propuesta de transacción de un cliente y le proporcionan sus firmas digitales después de su validación. Luego, se rellena el formato de la propuesta y se ejecuta el código de cadena de solicitud [18] con éxito.
Realizar pedidos		Un ordenante ordena propuestas de transacciones como transacciones de diferentes clientes para crear un nuevo bloque. Él firma el bloque con su firma digital y luego lo transmite a todos los pares, tanto los que respaldan como los que se comprometen en un canal.
Validación y compromiso		Después de recibir un nuevo bloque del solicitante, los pares verifican si cumple con los requisitos del pedido. Si es así, se respalda la política de respaldo y luego se valida la integridad de los datos en comparación con el resultado de la simulación en la fase de respaldo. Si no se encuentra ninguna discrepancia, un confirmador agrega el nuevo bloque al libro mayor y actualiza la base de datos estatal con los conjuntos de escritura de las transacciones.

tipo de algoritmo hash; y 1, 5 y 6 corresponden a MD5, SHA-256 y SHA-512, respectivamente. Salt es una cadena de caracteres alfanuméricos aleatorios de hasta 16 letras.

3. Esquema criptográfico

Antes de cargar los datos del paciente en el sistema EHR con el consentimiento del paciente, los datos se cifran utilizando una clave simétrica adecuada. Luego, la clave simétrica se cifra asimétricamente utilizando la clave pública del paciente y se adjunta a los datos cifrados. Este cifrado híbrido hace que el procedimiento sea eficiente en términos de velocidad y conveniencia porque el cifrado de datos de gran tamaño se puede realizar más rápidamente con una clave simétrica que con una clave asimétrica, mientras que esta última es más conveniente en el cifrado de claves criptográficas de tamaño pequeño.

Para leer los datos del paciente, un proxy los descarga del EHR correspondiente y los envía al receptor. Sin embargo, en caso de que el receptor sea diferente del paciente, la clave simétrica cifrada de los datos debe transformarse para que pueda ser descifrada por la clave privada del receptor. Para hacer esto, utilizamos un esquema de cifrado de proxy (Figura 2) en el que el paciente genera la clave de cifrado de proxy matemáticamente.

combinando su clave privada y la clave pública del receptor utilizando el algoritmo AFGH [20,21]. Después de recibir la clave de nuevo cifrado, el proxy vuelve a cifrar la clave simétrica para el receptor. En ese proceso, la clave simétrica no se revela al proxy. De lo contrario, el proxy debe enviar los datos al paciente para cifrarlos utilizando la clave pública del receptor.

4. Aplicación basada en web

Nuestro sistema proporciona una aplicación basada en web para que los clientes de cada hospital realicen solicitudes de acceso al libro mayor o al EHR. La aplicación basada en web es el programa de aplicación frontal disponible en un hospital o clínica. Un hospital puede tener un solo par o muchos pares según su escala, mientras que una clínica pequeña funciona como un cliente sin pares. Para identificar a los participantes en todo el sistema, se supone que los médicos de cada hospital tienen sus ECerts.

La aplicación basada en web ofrece interfaces de usuario basadas en web y funciones interactivas esenciales en la comunicación entre los participantes del sistema. Los pacientes lo utilizan para generar pares de claves para registrar e inscribir sus identidades en el sistema.

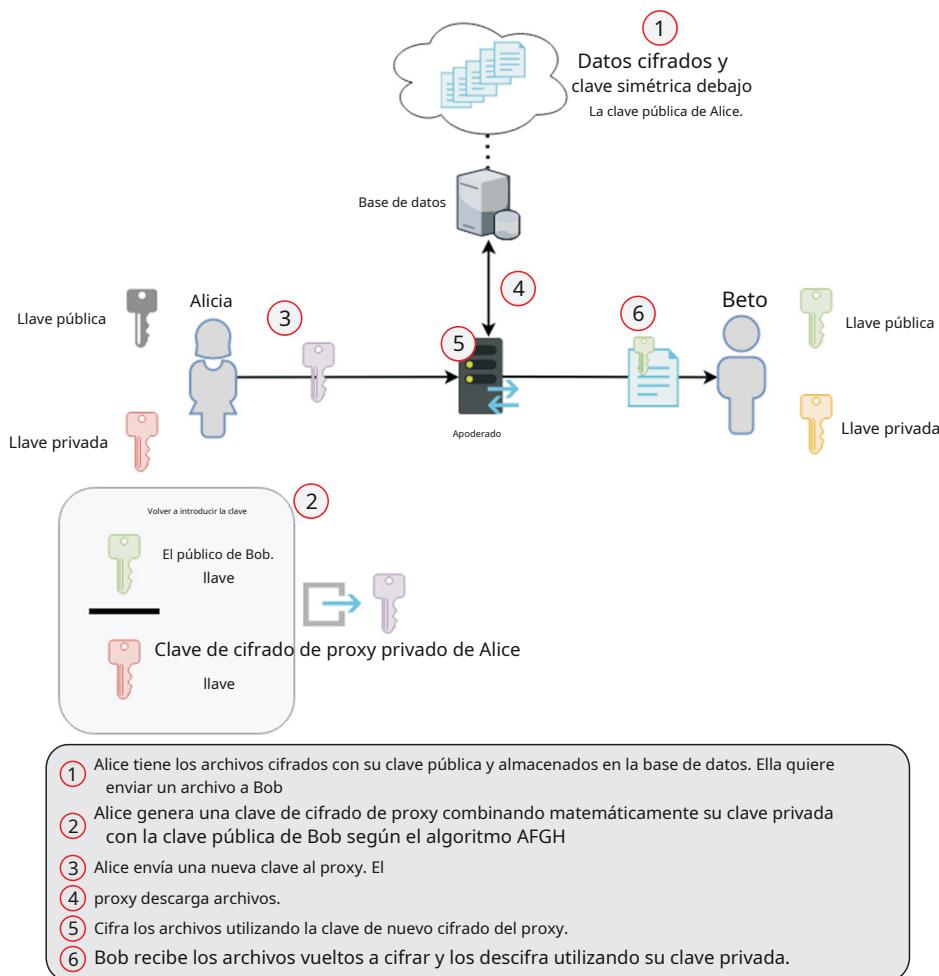


Figura 2. Esquema de recifrado de proxy.

para obtener ECerts. Además, pueden generar claves de recifrado de proxy y enviarlas al proxy. Por otro lado, el cliente utiliza esta aplicación basada en web para crear una propuesta de transacción y enviarla al sistema blockchain para tareas como identificar la identidad de un paciente y crear, cargar y compartir registros médicos, metadatos, etc.

III. Resultados

1. Códigos de cadena desarrollados

En nuestro sistema prototipo, instalamos cinco códigos de cadena con los que se ejecuta la lógica empresarial. Cada código de cadena tiene muchas funciones de programación y, por lo general, leen y actualizan el estado del libro mayor con toda la lógica empresarial contenida dentro de las funciones. En un sistema real, cada código de cadena debe lograr un acuerdo entre todos los hospitales miembros antes de implementarse en el sistema. La Tabla 3 presenta detalles de los códigos de cadena propuestos.

2. Escenarios de casos de uso

Simulamos casos de uso utilizando el sistema prototipo. En la Fig-

En las figuras 3 a 5, que describen una situación práctica, asumimos que una paciente, llamémosla Alice, visita el Hospital_A por primera vez. Allí, a Alice le diagnostican cáncer y su médico, el Dr. Bob, le recomienda ir al hospital central para ver a un especialista en cáncer. El Dr. Bob carga los registros de Alice con su consentimiento en el EHR del hospital. Luego, Alice se traslada al hospital central y el especialista en cáncer accede a los datos de Alice en el EHR que pertenece al Hospital_A.

1) Primera visita a un hospital

Alice hace una primera visita al Hospital_A (Figura 3). Para inscribirse en el hospital, proporciona su información demográfica o el número del seguro nacional a un empleado. Esta información se utilizará para registrarla en la fuente de identidad del paciente del hospital y emitirle un certificado electrónico. El ECert y la clave privada deben almacenarse en un dispositivo de almacenamiento seguro, por ejemplo, una tarjeta IC o una memoria USB. Después de emitir el ECert por parte de la autoridad certificadora (CA) local, el empleado debe almacenar el valor hash del eID de Alice y el ID del paciente individual en el libro mayor.

Tabla 3. Descripción de códigos de cadena instalados en el sistema prototipo

Códigos de cadena	Descripción
administrador de registros	Este es el código de cadena central del sistema, que participa en la ejecución de otros códigos de cadena, para simular propuestas de transacciones para la validación y respaldo de una propuesta. Este código de cadena ayuda al cliente a preparar, cargar y compartir los registros de un paciente.
identidad del paciente	Los clientes lo llaman para registrar y consultar la identidad de un paciente en el libro mayor. Los pacientes pueden encontrar una lista de transacciones de identidad que contienen sus visitas anteriores al hospital. Además, si los pacientes pierden sus ECerts, pueden proporcionar atributos identificables a los clientes para buscálos y recuperarlos. Los valores hash de eID y datos demográficos se pueden almacenar en el libro mayor para identificar a los pacientes. Dado que los pacientes recibirán diferentes ID de los hospitales que visitaron, este tipo de código de cadena también almacena y realiza consultas de ID de pacientes basadas en eID.
administrador de permisos	Esto funciona para autorizar el acceso de un tercero a los registros de los pacientes según el consentimiento del paciente. Consentimiento del paciente contiene una lista de identificaciones electrónicas a las que se les permite acceder, o condiciones de consentimiento previo integral, que un paciente coloca en una transacción como metadatos cuando los datos se registran en el libro mayor. Por ejemplo, un paciente puede compartir una parte específica de sus registros con una compañía de seguros que también participa en la red al incluir su identificación electrónica en la transacción.
carpeta personal	Esto ayuda a los médicos a recopilar todas las transacciones de un paciente. Proporciona funciones de consulta especiales para buscar las transacciones se basan en múltiples palabras clave, como el valor hash de un eID con Salt, ID de hospital o marca de tiempo.
Código de cadena de auditoría	Esto es para que los pares designados auditén los historiales de acceso de los registros de pacientes analizando el registro de acceso en el libro mayor. De este modo, los pacientes pueden darse cuenta de cómo sus datos han viajado entre las instituciones médicas y controlar si cada transferencia de datos se realizó de forma adecuada y cumpliendo con su consentimiento. Este código de cadena también puede producir estadísticas basadas en las actividades de los médicos, marcas de tiempo de las transacciones y metadatos de pacientes con datos demográficos.

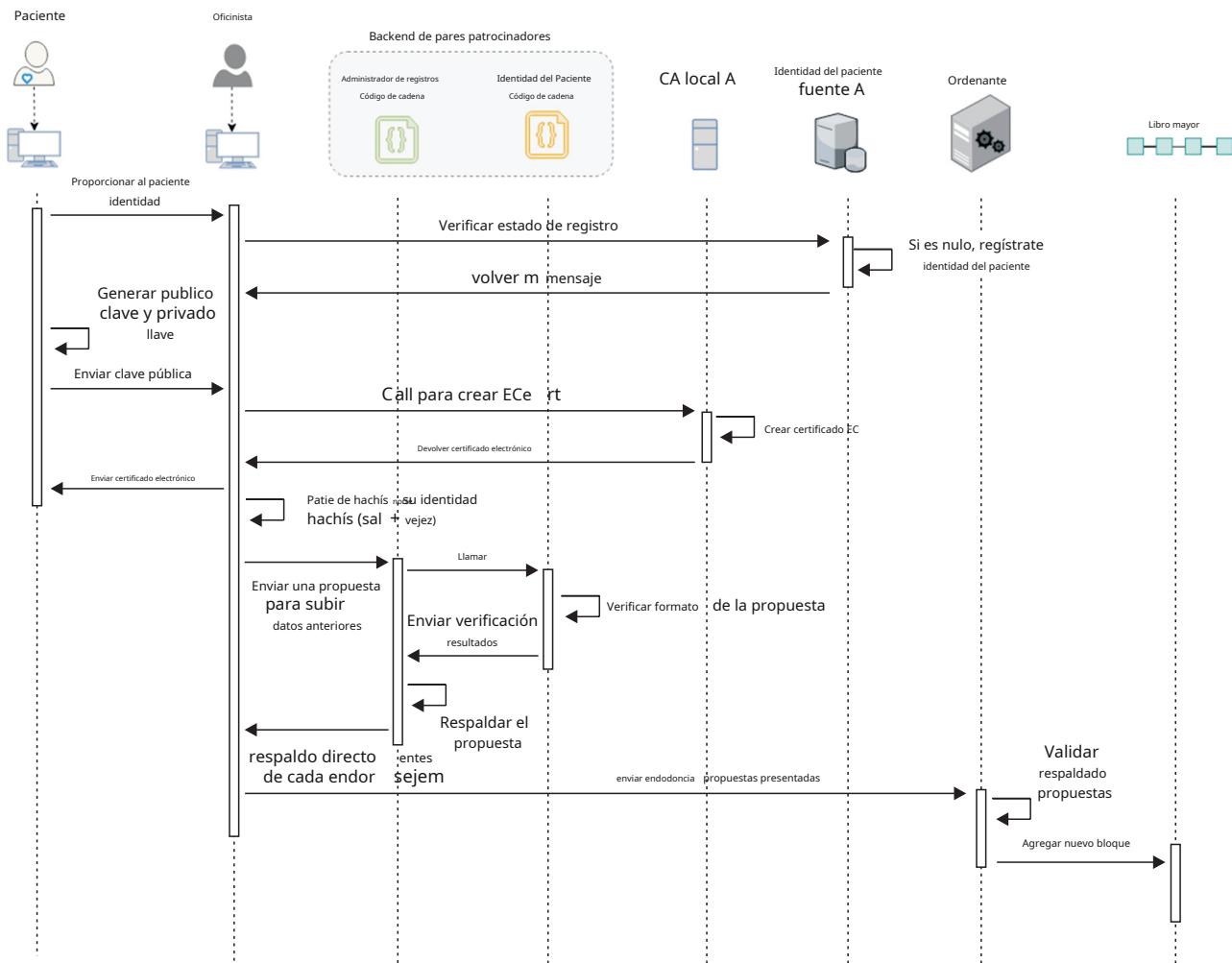


Figura 3. Primera visita a un hospital.

2) Cargar el registro del paciente con metadatos y consentimiento
 Cuando los registros de un paciente se cargan en el sistema EHR (Figura 4), Alice le da al médico su consentimiento con las condiciones para compartir sus registros con otros terceros o sus familiares. Luego, el médico cifra el registro de Alice utilizando una clave simétrica adecuada y esta vez cifra la clave utilizando la clave pública de Alice para adjuntarla al registro. Finalmente, el médico carga el registro de Alice en el sistema EHR de Hospital_A y escribe el consentimiento del registro y la dirección de la ubicación de los datos en el libro mayor.

3) Solicitar el registro del paciente

Alice va a ver a un especialista en el hospital central (Figura 5), donde se registra como nueva paciente, si es necesario, y proporciona su ECert previamente emitido en el Hospital_A. Al tratar a Alice, el médico desea obtener los registros anteriores de Alice, por lo que envía una propuesta de transacción de una solicitud para obtener los metadatos de los registros de Alice durante un período determinado y la identificación del hospital anterior. Luego, cada par que respalda simula el

propuesta de transacción que ejecuta códigos de cadena y devuelve cada resultado del código de cadena al proxy del hospital donde el médico ejecuta la aplicación del cliente. La aplicación compara los resultados de la consulta y, si todos coinciden, le permite al médico seleccionar los registros necesarios para hacer una lista de los registros del paciente que desea obtener. Después de recibir la lista, el proxy le pide a Alice que genere la clave de nuevo cifrado del proxy. Luego, el proxy descarga los registros de Alice en la lista de los EHR relevantes y vuelve a cifrar cada clave simétrica cifrada en cada registro mediante el nuevo cifrado. Después de eso, el apoderado envía los registros de Alice al médico.

3. Sistema prototípico

Se construyó un prototípico de sistema a pequeña escala para realizar pruebas en una red local con cuatro PC con Windows para que los pacientes utilicen la aplicación web para pacientes, cuatro PC con Linux para que los médicos utilicen la aplicación web para médicos y cuatro servidores proxy para cuatro hospitales. Además, utilizamos dos PC con Windows como EHR. La plataforma HLF se ejecutó en Docker para ejecutar códigos de cadena.

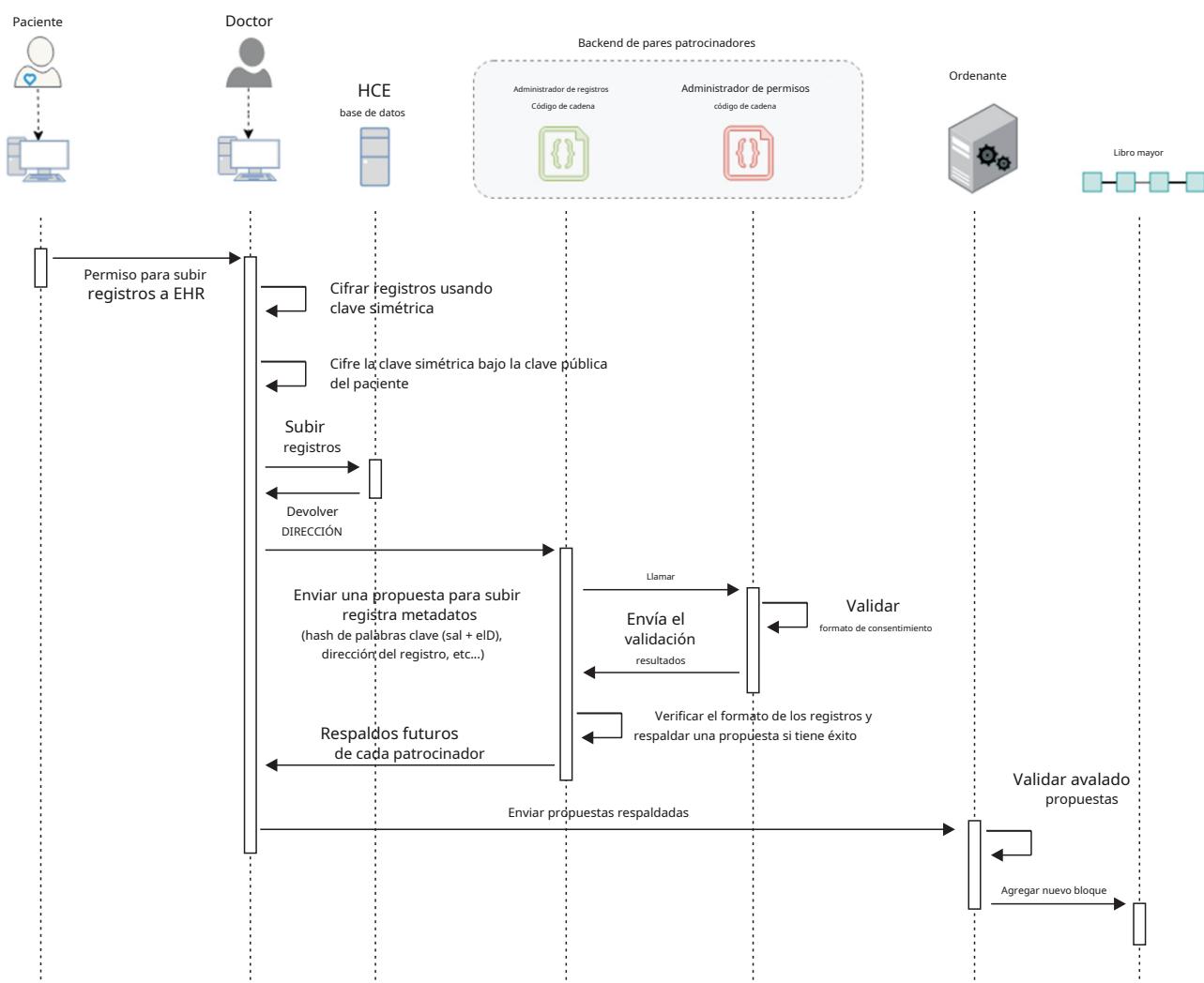


Figura 4. Carga de registro con metadatos y acceso de consentimiento. HCE: Historia Clínica Electrónica.

Para los registros EHR, tratamos con datos estandarizados, como datos de imágenes HL7/CDA y DICOM. Cambiamos la configuración del sistema con varios números de PC para evaluar el rendimiento, incluida la lógica del código de cadena. Como resultado, con un número cada vez mayor de PC se necesitaba un poco más de tiempo para consultar datos en una cadena de bloques, así como para cifrar y descifrar los registros y transferir archivos.

El prototipo anterior no es lo mismo que un entorno de trabajo real. El sistema y la funcionalidad del código de cadena pueden requerir modificaciones específicas para adaptarse a las políticas de privacidad del consorcio y los requisitos legales establecidos por la autoridad gobernante.

IV. Discusión

En la implementación del sistema, todos los pasos de verificación son esenciales por motivos de seguridad. Para proteger la privacidad del paciente, adoptamos el algoritmo Estándar de cifrado avanzado (AES).

ritmo para el cifrado de clave simétrica de los datos del paciente y el algoritmo de curva elíptica ElGamal (EC-ElGamal) para el cifrado de clave asimétrica de la clave simétrica en el esquema de recifrado proxy. El par de claves asimétricas también se utiliza para la firma de la propuesta de transacción. Sin embargo, con el fin de reforzar aún más la seguridad, un paciente puede tener otro par de claves para una firma diferente a la de las encriptaciones. El primero se genera utilizando la función HLF, el segundo importando una función de cifrado EC-ElGamal utilizando criptografía EC. Cuando un paciente elige tener dos pares de llaves, soporta una carga mayor para mantenerlas en secreto. En el caso de que un paciente pierda esta clave privada, se supone que se utiliza un sistema de custodia de claves para recuperar las claves perdidas o las claves simétricas del emisor del ECert o del hospital solo para descifrar los datos del paciente. Despues de todo, las claves recuperadas deben usarse temporalmente antes de que se emitan nuevas claves y un nuevo ECert para el paciente.

Realizamos hash de eID con salt para evitar transacciones de los registros

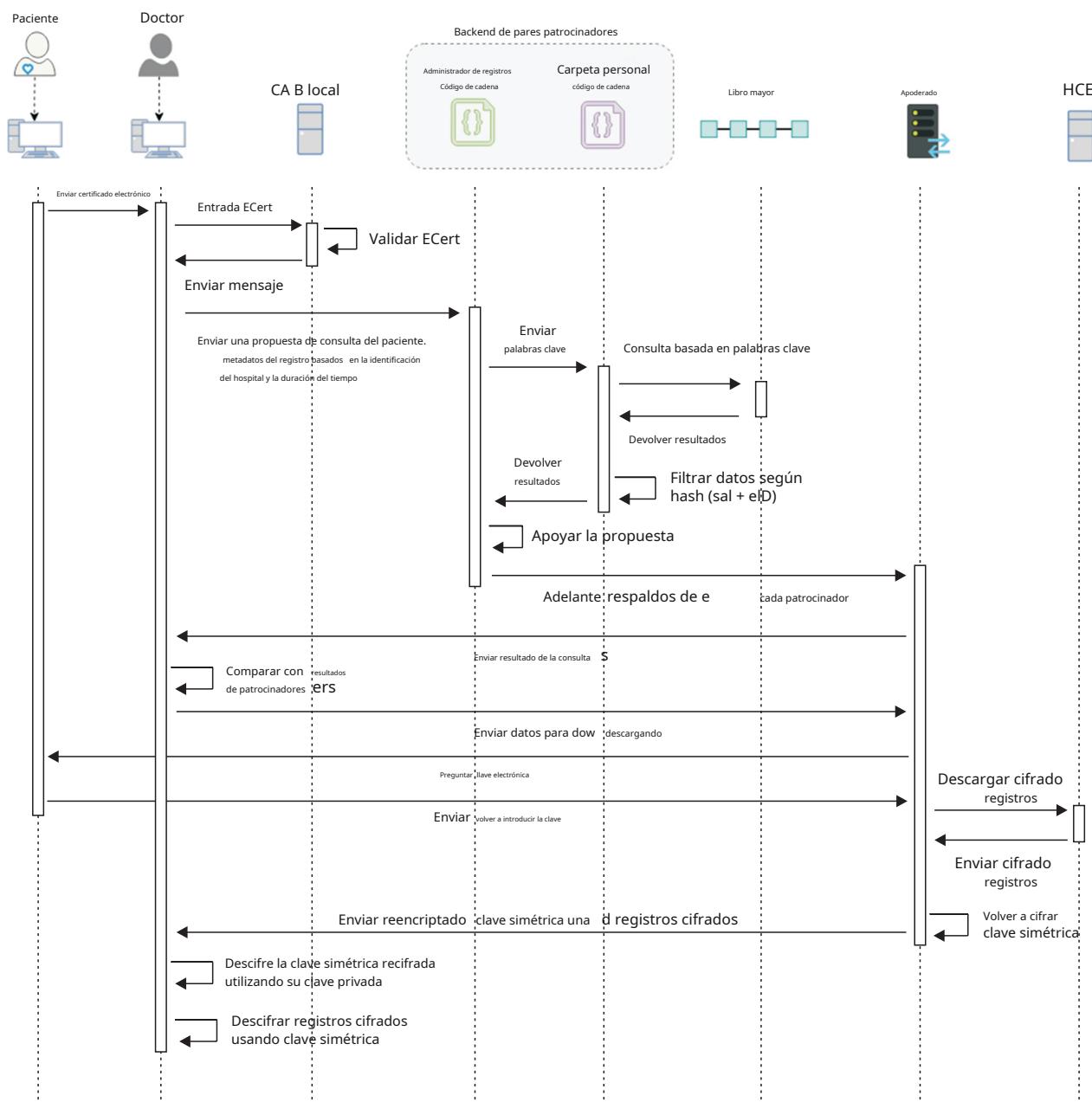


Figura 5. Solicitud de registros del paciente. CA: autoridad certificadora, EHR: Historia Clínica Electrónica.

relacionado con un paciente que tiene el mismo valor hash de eID con el que los registros del paciente podrían rastrearse de manera no deseada a lo largo del libro mayor. Mientras tanto, esta técnica provoca un mayor tiempo de procesamiento para encontrar un paciente que consulta los datos. Para acelerar el proceso, los médicos pueden ingresar muchas palabras clave de consulta relevantes para obtener los datos. Estas palabras clave incluyen no solo identificaciones electrónicas, sino también marcas de tiempo e identificaciones de hospitales.

Las funciones del proxy son conectar diferentes EHR a través de una red de comunicación segura, descargar los registros médicos y volver a cifrar los datos del paciente. Este esquema acorta el tiempo de procesamiento al transferir los datos de un paciente de forma segura; en caso contrario, los datos deberán ser enviados al paciente para

descifre usando la clave privada del paciente y cifre nuevamente usando la clave pública del receptor antes de enviarla de regreso al proxy y luego al receptor. Para el nuevo cifrado de proxy, adoptamos el algoritmo AFGH porque utiliza la clave pública del receptor en lugar de la clave privada como en el algoritmo BBS [22], donde la clave privada del receptor se crea y se usa transitoriamente solo para recibir los datos.

Para fortalecer la privacidad en el acceso a los registros, los pacientes pueden dar su consentimiento con condiciones en la transacción de los registros para compartirlos con terceros. Además, el libro de contabilidad conserva los eventos de intercambio de datos y la información de la persona relevante, lo que facilita el procedimiento de auditoría.

Ha habido varios proyectos para establecer un sistema de intercambio de información médica basado en blockchain. Entre ellos, MedRec [23] es un estudio inicial que aplica la plataforma privada Ethereum a los EMR. En Ethereum, un programa ejecutable que se ejecuta en la red se denomina contrato inteligente en lugar de código de cadena. Ethereum requiere mecanismos de minería para sostener el libro mayor distribuido, que es un proceso retardado en el que los mineros compiten en prueba de trabajo, aunque no es difícil hacer que una plataforma privada tenga un tiempo de bloque corto de menos de 10 segundos. Es necesario incentivar a las partes interesadas médicas, como investigadores, autoridades de salud pública, etc., para que participen activamente como mineros. Para abordar estos problemas, MedRec 2.0 se encuentra actualmente en desarrollo [24].

Ancile [13] es otro sistema basado en blockchain que utiliza la plataforma privada Ethereum, que aplica una técnica similar a la nuestra para la gestión de registros médicos, adoptando el concepto dentro y fuera de la cadena. Ancile utiliza servidores proxy distribuidos para el recifrado, llamado recifrado ciego, dividiendo el texto cifrado para el recifrado entre múltiples nodos.

Por otro lado, Dubovitskaya et al. [25] utiliza HLF en el sistema de nube. En este sistema, la estructura de datos consta de un par de clave y valor. La clave es un hash de una combinación de la clave simétrica y la información de identificación única (UII) del paciente, y el valor son los metadatos del registro. Para reducir la vulnerabilidad del sistema, los pacientes cifran cada dato utilizando diferentes claves simétricas. Sin embargo, esto implica una gran carga de gestión de claves, de modo que los pacientes deben elegir la clave simétrica correspondiente para generar un número de clave cada vez que consultan los datos.

Nuestro sistema es una red de consorcio. Si otras instituciones médicas desean acceder a esta red, deben realizar una solicitud para registrarse como miembro de esta red. En caso contrario, una institución no miembro puede comunicarse a través de las instituciones miembros. Los pares son los elementos de confianza de cada institución médica. Necesitan fortalecer su propia seguridad para proteger a sus pares del acceso ilegal. Al mismo tiempo, cada institución médica debe acordar la lógica del código de cadena antes de implementarlo en el sistema. Por lo tanto, nuestro sistema blockchain también puede ejecutarse eficazmente en el sistema de nube, aunque su punto de vista fundamental es opuesto en términos de descentralización. La computación en la nube puede proporcionar una solución al problema del tamaño de la cadena de bloques: el tamaño del libro mayor aumenta gradualmente con el tiempo y los pares tendrán dificultades para conservarlo y procesarlo.

En conclusión, nuestro sistema puede utilizarse para constituir un sistema EHR a gran escala. Es configurable de manera flexible para ser una capa superior de los sistemas EHR existentes para fortalecer la seguridad en el manejo.

Gestión e intercambio de registros médicos. Nuestro sistema asume las funciones de identificador de paciente, registro de acceso del administrador y registro de registros de pacientes. Aunque nuestro sistema no ofrece incentivos explícitos a los participantes como lo hacen otros sistemas basados en blockchain mediante la emisión de una criptomoneda, también beneficiará a los usuarios y a las partes interesadas, incluidos los proveedores de servicios de salud y el gobierno. Esperamos que nuestra investigación pueda ayudar a los pacientes a encontrar sus historiales médicos más fácilmente cuando visitan otros hospitales. Como trabajo futuro, vamos a probar nuestro sistema en un entorno hospitalario real. Nos prepararemos para lidiar con datos no estandarizados en una prueba de campo del mundo real.

Conflictos de intereses

No se informó ningún posible conflicto de intereses relevante para este artículo.

ORCID

Dara Tith (<http://orcid.org/0000-0003-4372-7640>) Joong-Sun Lee (<http://orcid.org/0000-0002-6976-6472>) Hiroyuki Suzuki (<http://orcid.org/0000-0002-5028-5388>) WMAB Wijesundara (<http://orcid.org/0000-0002-7228-524X>) Naoko Taira (<http://orcid.org/0000-0001-6169-8957>)
Takashi Obi (<http://orcid.org/0000-0001-9430-2728>) Nagaaki Ohyama (<http://orcid.org/0000-0002-4297-2575>)

Referencias

1. Greenhalgh T, Hinder S, Stramer K, Bratan T, Russell J. Adopción, no adopción y abandono de un registro médico electrónico personal: estudio de caso de Health-Space. *BMJ* 2010;341:c5814.
2. Pylypchuk Y, Johnson C, Henry J, Circean D. Variación en la interoperabilidad entre los hospitales de cuidados intensivos no federales de EE. UU. en 2017. *ONC Data Brief* 2018;(42):1-15.
3. Alianza para la salud CommonWell. Acerca de CommonWell [Internet]. [lugar desconocido]: CommonWell Health Alliance; c2020 [citado el 10 de enero de 2020]. Disponible en: <https://www.commonwellalliance.org/about/>.
4. Alianza para la salud CommonWell. Casos de uso y especificaciones [Internet]. [lugar desconocido]: CommonWell Health Alliance; c2020 [citado el 10 de enero de 2020]. Disponible en: <https://www.commonwellalliance.org/connect-tothenetwork/use-cases-and-specifications/>.
5. van der Linden H, Kalra D, Hasman A, Talmon J. Sistemas EHR interorganizacionales preparados para el futuro: una revisión de

- las cuestiones relacionadas con la seguridad y la privacidad. *Int J Med Inform* 2009;78(3):141-60.
6. Keris diputada. Una caja de Pandora: la pista de auditoría del EMR [Internet]. [lugar desconocido]: Blog de descubrimiento de EMR; 2017 [citado el 10 de enero de 2020]. Disponible en: <https://www.emrdiscoveryintel.com/single-post/A-Pandoras-Box>.
 7. Walsh T, Miaoulis W. Auditorías de privacidad y seguridad de la información médica electrónica. *JAHIMA* 2014;85(3):54-9.
 8. Guía de cumplimiento de HIPAA [Internet]. [lugar desconocido]: La Guía HIPAA; c2017 [citado el 10 de enero de 2020]. Disponible en: <https://www.hipaaguide.net/hipaa-compliance-guide/>.
 9. Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, et al. Una taxonomía de sistemas basados en blockchain para el diseño de arquitectura. Actas de la Conferencia Internacional IEEE 2017 sobre Arquitectura de Software (ICSA); 3-7 de abril de 2017; Gotemburgo, Suecia. pag. 243-52.
 10. Sousa J, Bessani A, Vukolic M. Un servicio de pedidos bizantino tolerante a fallas para la plataforma blockchain de tejido Hyperledger. Actas de la 48^a Conferencia Internacional Anual IEEE/IFIP sobre Sistemas y Redes Confiables (DSN); 25-28 de junio de 2018; Ciudad de Luxemburgo, Luxemburgo. pag. 51-8.
 11. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Tejido Hyperledger: un sistema operativo distribuido para cadenas de bloques autorizadas. Actas de la 13^a Conferencia EuroSys; 23-26 de abril de 2018; Oporto, Portugal.
 12. Tejido Hyperledger. ¿Qué es una cadena de bloques [Internet]? [lugar desconocido]: Hyperledger; c2019 [citado el 10 de enero de 2020]. Disponible en: <https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html>.
 13. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: marco de preservación de la privacidad para el control de acceso y la interoperabilidad de registros médicos electrónicos utilizando tecnología blockchain. *Sustain Cities Soc* 2018;39:283-97.
 14. Roehrs A, da Costa CA, da Rosa Righi R. OmniPHR: un modelo de arquitectura distribuida para integrar registros de salud personales. *J Biomed Inform* 2017;71:70-81.
 15. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distribuyó tecnologías de contabilidad para aplicaciones biomédicas y de atención médica. *J Am Med Inform Assoc* 2017;24(6):1211-20.
 16. Manzoor A, Liyanage M, Braeke A, Kanhere SS, Ylianttila M. Esquema de cifrado de proxy basado en Blockchain para el intercambio seguro de datos de IoT. Actas de la Conferencia Internacional IEEE de 2019 sobre Blockchain y Criptomonedas (ICBC); 2019 14-17 de mayo; Seúl, Corea. pag. 99-103.
 17. Thakkar P, Nathan S, Viswanathan B. Evaluación comparativa del rendimiento y optimización de la plataforma blockchain de tejido Hyperledger. Actas del 26º Simposio internacional del IEEE sobre modelado, análisis y simulación de sistemas informáticos y de telecomunicaciones (MAS-COTS); 25-28 de septiembre de 2018; Milwaukee, Wisconsin. pag. 264-76.
 18. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY. Contratos inteligentes habilitados para blockchain: arquitectura, aplicaciones y tendencias futuras. *IEEE Trans Syst Man Cybern Syst* 2019;49(11):2266-77.
 19. Preneel B. Funciones hash criptográficas: teoría y práctica. En: Gong G, Gupta KC, editores. *Progresos en criptología – INDOCRYPT 2010*. Heidelberg, Alemania: Springer; 2010. pág. 115-7.
 20. Thangam V, Chandrasekaran K. Nuevo cifrado de proxy basado en curva elíptica. Actas de la Segunda Conferencia Internacional sobre Tecnologías de la Información y las Comunicaciones para Estrategias Competitivas (ICTCS); 4 y 5 de marzo de 2016; Udaipur, India. pag. 1-6.
 21. Chow SS, Weng J, Yang Y, Deng RH. Nuevo cifrado de proxy unidireccional eficiente. En: Bernstein DJ, Lange T, editores. *Progresos en criptología – AFRICACRYPT 2010*. Heidelberg, Alemania: Springer; 2010. pág. 316-32.
 22. Ateniese G, Fu K, Green M, Hohenberger S. Esquemas de cifrado de proxy mejorados con aplicaciones para proteger el almacenamiento distribuido. *ACM Trans Inf Syst Secur* 2006;9(1): 1-30.
 23. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: uso de blockchain para el acceso a datos médicos y la gestión de permisos. Actas de la Segunda Conferencia Internacional sobre Datos Abiertos y Big Data (OBD); 22-24 de agosto de 2016; Viena, Austria. pag. 25-30.
 24. MedRec [Internet]. Cambridge (MA): Laboratorio de Medios del MIT; c2019 [citado el 10 de enero de 2020]. Disponible en: <https://medrec.media.mit.edu/technical/>.
 25. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Intercambio seguro y confiable de registros médicos electrónicos mediante Blockchain. *AMIA Annu Symp Proc* 2018;2017: 650-9.