Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Maestría en Seguridad Informática

Tesis de maestría

Título

Cadena de bloques: Diseño de una solución para el control de Historias Clínicas Electrónicas enfocado en la seguridad de la información.

Autor: Ing. Joffre Aguirre

Director de Tesis: Dr. Pedro Hecht

Año 2020

Cohorte 2016

Declaración Jurada:

"Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual"

FIRMADO

Joffre Armando Aguirre Regato

PASAPORTE: 091835743

Tabla de contenidos

Introducción

La Historia Clínica Electrónica (HCE) desde su concepción no fue diseñada para ser manejada como un documento multi institucional lo cual limita el contexto de la información a las instituciones donde se atiende al paciente. En consecuencia, todos los eventos de un paciente se encuentran aislados en las diferentes instituciones de salud donde ha sido atendido a lo largo de su vida.

Varias alternativas de solución para HCE de código abierto se tienen a la mano como OpenEMR, OpenMRS, VistA, GNUmed. Desde el punto de vista de seguridad de la información existen varios pilares fundamentales que se deben analizar para un sistema de HCE: una arista del problema es mantener la privacidad y confidencialidad de los datos del paciente, otra arista es la propiedad sobre los datos, y por último la disponibilidad e integridad de los datos del paciente sin importar la ubicación geográfica o el proveedor de servicios de salud. Aquí nos debemos formular las siguientes preguntas respecto a los datos: ¿son propiedad de la institución de salud o del paciente?, ¿Deben ser ofrecidos para investigaciones en el campo de salud sin afectar la seguridad de la información y cómo?, ¿Cómo un paciente puede llevarlos a través de toda la red de proveedores de servicios o como los proveedores deben facilitarlos entre sí?, ¿Quién garantiza la seguridad de la información o se hace responsable de la gestión de los datos médicos?

Además, se puede evidenciar la existencia de muchas personas y entes que pueden manipular la información, he aquí las siguientes inquietudes que aclararemos para diseñar nuestra propuesta:

- El propietario de la información. El propietario de la información es el paciente, el especialista o medico de salud, el centro de salud u hospital donde se atiende el paciente, o por último el ministerio de salud de una región o país que es responsable de brindar salud a todos los ciudadanos.
- Bajo qué ley se puede amparar los datos de salud. En algunos países existen leyes de “habeas data”, protección de datos en

general y propias de salud, en nuestro caso definiremos para Ecuador cuales leyes podrían regir para el diseño.

- Un modelo en la cadena de bloques que garantice la seguridad de los datos de salud.

Objetivo general

La presente propuesta de trabajo tiene como objetivo diseñar una solución sobre una cadena de bloques autorizada o *Blockchain permissioned* que cumpla con los requisitos de las reglas de seguridad y privacidad establecidas por la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA) y el Reglamento General de Protección de Datos (RGPD) para soportar el control de la HCE de un paciente.

Objetivos específicos

Se realizará un análisis de los requerimientos que deben cumplir los sistemas de HCE, a través de un paradigma orientado a la seguridad de la información, revisando los siguientes puntos:

- Leyes actuales que protegen los datos de los pacientes.
- Modelos de distribución de estos datos.
- Esquemas de seguridad actuales.
- Recomendaciones de otros gobiernos y capacidades de los sistemas, todo esto acotado específicamente para la república del Ecuador.

Los cuáles serán soportados por los siguientes diseños:

- Tipo de Blockchain: privada o pública.
- Grupo de interesados para el diseño.
- Requisitos del diseño.
- Mapa conceptual del diseño.
- Consideraciones para el diseño.
- Diseño final de la solución sobre la cadena de bloques.

Como excepciones, no se desarrollará ni implementará ningún sistema, solo se entregará el análisis y diseño desde el enfoque de seguridad de la información.

Desarrollo

1. Marco Teórico

1.1 Registros de Salud Electrónicos

Los *Electronic Health Record* (EHR) son registros electrónicos de salud y típicamente son mantenidos por un hospital, una autoridad de salud o un ministerio regional de salud e incluyen una variedad de orígenes/repositorios de datos del paciente [1]. Mientras que los *Electronic Medical Record* (EMR) son registros únicos creados por los doctores o prestadores de salud, separando conceptos, se puede decir que la unión de muchos EMR de doctores de diferentes especialidades o diferentes prestadores de salud forman un EHR.

Como función central se debe notar que EHR y EMR es información privada y confidencial sensible para el diagnóstico y tratamiento en la atención de salud, la cual debe distribuirse con frecuencia y compartirse entre pares, como proveedores de salud, farmacias, investigadores, familiares de pacientes, compañías de seguros, entre otros. En consecuencia, se debe mantener actualizada los EHR de un paciente, para almacenar o compartir datos entre múltiples entidades manteniendo el control de acceso a través de numerosas autorizaciones, lo cual complica el proceso del tratamiento de un paciente.

Los EHR presentan nuevos retos para la privacidad y seguridad debido a que existen roles como proveedores de salud, custodios de la información, administradores de la información, consumidores de la información y terceros. Para un mejor entendimiento definiremos como:

Un proveedor de salud es cualquier especialista, institución de cuidado, centro o cuidado ambulatorio que provea servicios de salud a un paciente. Un custodio de la información puede ser cualquiera que genere un EMR o un EHR. Adicional, un administrador de la información puede ser cualquier proveedor de salud que mantenga la información segura, confiable, disponible y puede ser un especialista de salud, institución de salud o un ministerio.

Un consumidor de la información puede ser cualquier otro especialista o institución de salud que solicita acceso a la EHR del paciente, inclusive el

mismo paciente. Por último, un tercero es cualquier ente que tiene acceso a la información con fines de investigación médica, estadísticas de salud, o una simple revisión de rutina sobre un equipo móvil de un especialista en un borde fronterizo [2].

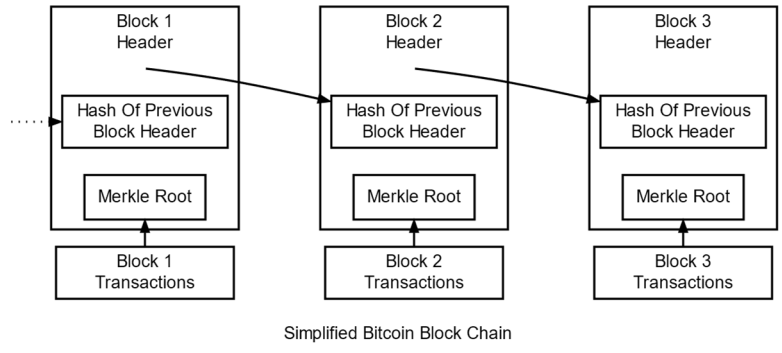
Para mejor entendimiento de nuestra propuesta de aquí en adelante los registros médicos generados como eventos: tomas de datos, órdenes de laboratorio, etc. serán llamados EHR o EMR y la suma de todos estos se conocerá como HCE.

1.2 Cadena de Bloques

Satoshi Nakamoto, la persona o grupo desconocido detrás de Bitcoin, describió cómo la tecnología Cadena de Bloques (*Blockchain*), una estructura distribuida y enlazado punto a punto [3]. La Cadena de Bloques provee un libro mayor de registro de bloques de transacciones ordenadas en forma cronológica. Este sistema es usado para solucionar el problema del doble gasto y prevenir la modificación de transacciones previas [4].

Los nodos de la red o mineros son responsables de vincular los bloques entre sí en orden cronológico con cada bloque que contiene el hash del bloque anterior para crear una cadena de bloques. Por lo tanto, la estructura de la Cadena de Bloques logra contener un registro robusto y auditable de todas las transacciones como se muestra en la figura abajo.

Ilustración 1. Modelo simplificado de la Cadena de Bloques



Fuente: [4]

Una Cadena de Bloques puede ser considerada como una base de datos distribuida que se organiza como una lista de bloques ordenados, donde los bloques comprometidos son inmutables. Se debe tener especial cuidado

en el término “base de datos distribuida”, lo que realmente se plantea es una base de datos replicada en todos los nodos. En otras palabras, cada nodo tiene una copia exacta de la base que puede existir en cualquier otro nodo.

Basado en el control de acceso a la Cadena de Bloques se puede obtener las siguientes categorías:

1.2.1 Implementación de Cadena de Bloques sin Autorización.

Las cadenas de bloques sin autorización son sistemas abiertos y descentralizados donde cualquier usuario puede unirse o salirse con permisos de lectura y escritura, Además, todas las identidades de los participantes son pseudónimas o incluso anónimas y cada usuario puede agregar un nuevo bloque a la cadena participando en el algoritmo de consenso de la red. El caso de Bitcoin [5], Ethereum [6] son ejemplos de Cadenas de Bloques sin permisos las cuales permiten que cualquiera cree y ejecute algoritmos de cierta complejidad en su plataforma

Lo que Ethereum proporciona es una Cadena de Bloques con un lenguaje de programación Turing completo que se puede usar para crear Contratos Inteligentes y se puede usar para codificar funciones de transición de estado, permitiendo a los usuarios crear Contratos Inteligentes, simplemente escribiendo la lógica en unas pocas líneas de código [7].

1.2.2 Implementación de Cadena de Bloques con Autorización.

Una cadena de bloques con autorización tiene una entidad central que maneja la identidad de los participantes en la red y el algoritmo de consenso está restringido a un conjunto de nodos en la red. Además, proporciona una manera de proteger las interacciones entre un grupo de entidades que tienen un objetivo común pero que no confían plenamente entre sí, como las empresas que intercambian fondos, bienes o información. Al confiar en las identidades de los pares, una cadena de bloques con permiso puede utilizar el consenso tradicional tolerante a fallas bizantinas (BFT) [8].

Hyperledger Fabric es una cadena de bloques autorizada para uso comercial. Es de código abierto y se basa en estándares, ejecuta contratos inteligentes definidos por el usuario, admite características sólidas de

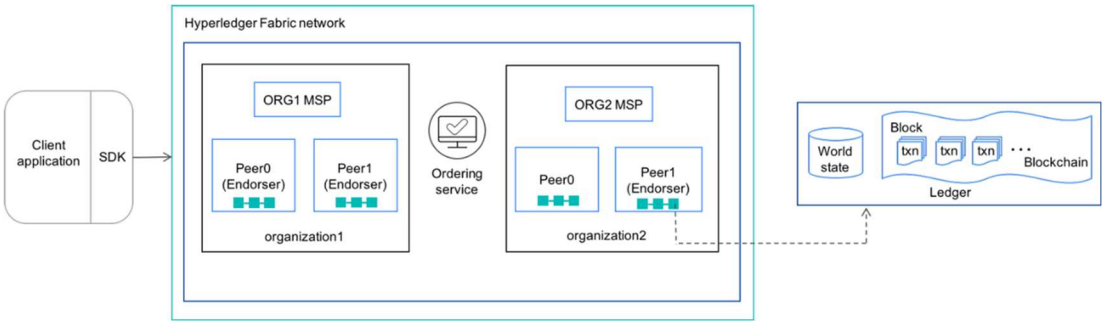
seguridad e identidad. Por último, utiliza una arquitectura modular con protocolos de consenso personalizados e intercambiables [9].

Hyperledger Fabric

Nos permitimos una explicación más amplia de la implementación de la cadena autorizada Hyperledger Fabric [10] debido a que la usaremos como Framework para nuestro diseño.

Hyperledger Fabric [10] es una implementación de código abierto para redes privadas y con permisos, en la que sus miembros conocen las identidades y los roles de los otros miembros. Con diseño modular que permite acoplar componentes, como la base de datos de libros contables, el mecanismo de consenso y los servicios de suscripción. Además, proporciona seguridad, escalabilidad y confidencialidad. Consta de los siguientes componentes básicos [10] tal como se muestra en la figura de abajo:

Ilustración 2. Componentes de red Hyperledger



Fuente: [11]

- Activos. Un activo es cualquier cosa que tenga valor, posee estado y propiedad. En Hyperledger Fabric los activos se representan como una colección de pares clave-valor.
- Libro contable compartido o *Ledger*. El *Ledger* registra el estado y la propiedad de un activo. El libro contable está formado por dos componentes:
    - El *world state* describe el estado del Ledger en un momento determinado. Es la base de datos del libro contable.
    - El *blockchain* es un histórico del registro de transacciones.
- Contrato inteligente o *chaincode*. *Chaincode* es un software que define los activos y sus transacciones relacionadas; en otras

palabras, contiene la lógica empresarial del sistema. El *chaincode* se invoca cuando una aplicación tiene que interactuar con el Ledger. El *chaincode* se puede escribir en Golang o Node.js.

- Nodos del par o *Peer*. Los *Peers* son elementos básicos de la red porque alojan los *Ledger* y los *chaincode*. Los *peers* ejecutan el *chaincode*, acceden a datos del *ledger*, respaldan transacciones e interactúan con aplicaciones. Algunos *peers* pueden ser *endorsing peers* o pares endosadores. Cada *chaincode* puede especificar una política de aprobación, que define las condiciones necesarias y suficientes para aprobar una transacción válida.
- Canal o *Channel*. Los canales son estructuras lógicas formadas por una colección de *peers*. Esta capacidad permite que un grupo de pares creen un ledger separado.
- Organizaciones. Hyperledger Fabric se construye a partir de los *peers* de diferentes organizaciones que forman parte de la red. La red existe porque las organizaciones contribuyen con sus recursos. Los *peers* tienen una identidad (certificado digital) asignada por un Proveedor de Servicios de Suscripción de la organización a la que pertenecen. Los peers de diferentes organizaciones pueden estar en el mismo canal.
- *Membership Service Provider* o Proveedor de Servicios de Suscripción (MSP). El MSP se implementa como una Autoridad Certificadora o CA para gestionar los certificados que se utilizan para autenticar la identidad y los roles de los miembros de la red. En la red Hyperledger Fabric solo se pueden realizar transacciones de identidades conocidas lo que permite que Hyperledger Fabric sea una red privada y con permisos.
- *Ordering Service* o Servicio de pedido. El *ordering service* empaqueta las transacciones en bloques que se entregarán a los *peers* a través de un canal. Garantiza la entrega de transacciones en la red comunicándose con los *peers* de aprobación u *orderer peers*. Los mecanismos de consenso soportados para el *ordering service* son Raft, Kafka y SOLO.

La red de Hyperledger Fabric [11] funciona como *backend* con una aplicación de *frontend* para comunicarse con la red. Los kits de desarrollo de software o *Software Development Kit* (SDK) como Nodejs SDK y Java SDK le ayudan a establecer la comunicación entre el *frontend* y el *backend*. El SDK proporciona una forma de ejecutar el *chaincode* del usuario, de realizar transacciones en la red, de supervisar eventos, etc.

- Para escribir una aplicación de *blockchain*, es necesario:
- Escribir el *chaincode* en un lenguaje de programación compatible, como Go o JavaScript.
- Implementar el *chaincode* en la red de Hyperledger Fabric.
- Desarrollar una aplicación del cliente con un SDK.

El flujo de una transacción en una red Hyperledger Fabric [11] a muy alto nivel se describe a continuación:

- El cliente se conecta a una red de Hyperledger Fabric a través de Nodejs o de Java SDK. La aplicación cliente crea una transacción o *proposal* y la envía al *endorsement peer*.
- El *endorsement peer* verifica la firma del cliente, simula la transacción y envía una firma de la aprobación o *endorsement*.
- Si llega firmada la transacción a la aplicación con la firma de los *endorsement peers* y cumple la política del *chaincode*, la aplicación cliente la envía al *ordering service*. En caso contrario, la transacción se cancela.
- El *ordering service* entrega una transacción a los *peers*. Todos los *peers* verifican y aplican la misma secuencia de transacciones. De tal forma, que actualizan su *Ledger*. Como el consenso es liderado por el *ordering service* no permite las bifurcaciones o *forks* que se observan en *blockchains* no autorizadas.

2. Marco Legal

2.1 Leyes Ecuatorianas

Para el Ecuador existen las siguientes leyes:

La Constitución de la República del Ecuador establece en su artículo 66 Numeral 19 “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley” [12]. El artículo en la constitución establece un principio sobre la protección de datos, pero no define “datos de carácter personal” y no establece quien es el titular o dueño de la información.

También establece en la sección quinta “hábeas data” articulo 92 “Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados” [12].

Se puede notar que no incluye la definición de dato sensible, tampoco da una definición clara de las medidas de seguridad necesarias para salvaguardar los datos sensibles. En conclusión, las dos leyes son de carácter general pero no existe una ley específica vigente que explique las definiciones de datos público, privado, sensible y tampoco existe los procesos o procedimientos para garantizar el acceso, el procesamiento, la distribución o la autorización por parte del titular de los datos.

La Ley Orgánica de Salud establece en su capítulo 3 articulo 7 literal f y h, "Toda persona, sin discriminación por motivo alguno, tiene en relación a salud derecho a una historia clínica única redactada en términos precisos, comprensibles y completos, así como la confidencialidad respecto de la información en ella contenida y a que se le entregue su epicrisis" y "No ser objeto de pruebas, ensayos clínicos, de laboratorio o investigaciones, sin su conocimiento y consentimiento previo por escrito; ni ser sometida a pruebas o exámenes diagnósticos, excepto cuando la ley expresamente lo determine o en caso de emergencia o urgencia en que peligre su vida" [13].

Existe un Acuerdo Ministerial 9 o Reglamento para el Manejo de Historia Clínica Electrónica que tiene por objeto disponer la implementación de la Historia Clínica Electrónica, así como definir los lineamientos de su aplicación, en los establecimientos prestadores de servicios de salud, en el Ecuador y en temas de seguridad de la información establece en el artículo 7 “El uso y manejo de la Historia Clínica Electrónica se rige bajo los principios de seguridad, integridad de la información, autenticidad, confidencialidad, exactitud, inteligibilidad, no repudio, conservación, disponibilidad, pertinencia y acceso” [14]. Además, este acuerdo establece a la HCE como:

La Historia Clínica Electrónica es un registro electrónico personal, resultado de una atención de salud, que se encuentra contenido en una base de datos, generada mediante programas informáticos, y certificada con la firma electrónica del profesional de la salud. Sin perjuicio de que los establecimientos prestadores de servicios de salud sean custodios de la Historia Clínica Electrónica, los pacientes son los titulares de los datos que respecto de ellos se almacene en la Historia Clínica Electrónica. [14]

Ecuador no tiene una Ley de protección de Datos personales, pero existe un borrador de proyecto que tiene como objetivo regular el ejercicio del derecho a la protección de datos personales siguiendo los lineamientos del modelo europeo. Para nuestra tesis notamos en el proyecto “Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los datos personales” [15] en el artículo 4 establece los siguientes lineamientos para los datos de salud:

- Establece como titular de los datos a la personal natural cuyos datos personales son objeto de tratamiento de datos. Pero,

entrega una definición de titular no de propietario de la información.

- Clasifica como “Dato Sensible” [15] a los datos genéticos, de salud y a la vida sexual u otro dato vinculado con la intimidad del titular. Pero lamentablemente no define que es “intimidad” ante la ley.
- En el título V Transferencia internacional de datos artículo 21 plantea la excepción “Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico”. Por consiguiente, no es necesario en este caso la autorización expresa e inequívoca del titular de los datos para su transferencia.
- En el titulo VI Infracciones y Sanciones artículo 25 literal 2 indica como una infracción grave “Recabar y tratar datos sensibles, sin consentimiento expreso del titular y no guardar la respectiva confidencialidad”.

El proyecto de ley busca que todos los involucrados observen y respeten los siguientes principios: legalidad, pertinencia, veracidad, consentimiento informado, confidencialidad y reserva. Por ejemplo, los datos personales de una persona deben estar en una base de datos inscrita por un responsable de la información de la compañía X; los datos no pueden ser usados para fines distintos a los que motivaron su obtención; los datos recolectados deben ser veraces y no excesivos u obtenidos de forma fraudulenta; el titular de los datos deberá entregar su consentimiento libre e inequívoco previo a la entrega de los mismos, salvo ciertas excepciones; responsable como usuario de los datos deberán garantizar la confidencialidad e integridad de los datos siempre permitiendo acceso al titular de los datos; se prohíbe la difusión a terceros [15].

2.2 Leyes Extranjeras

2.2.1 HIPAA

Esta norma reglamenta específicamente los datos de salud de las personas, pero aplica únicamente para los Estados Unidos de América,

aunque por su especificación muchos proveedores de salud, proveedores de sistemas y seguros aplican su cumplimiento como una buena práctica alrededor del mundo. Como cita Aguirre “La *Health Insurance Portability and Accountability Act of* 1996 (HIPAA) o ley 104-191, protege el uso y la divulgación de la información de salud de las personas” [4], y se compone de:

La Norma de Privacidad. La cual aborda el uso y divulgación de la información de salud de los individuos denominada “información de salud protegida” por parte de las organizaciones sujetas a la Regla de Privacidad, las cuales se denominan entidades cubiertas. La Regla de Privacidad llama a está “información de salud protegida” o *Protected Healt Information* (PHI) la “información de salud identificable individualmente” e incluye datos demográficos y se relaciona con: la salud o la condición física o mental en el pasado, presente o futuro del individuo; la prestación de atención de salud a la persona; y el pago en el pasado, presente o futuro por la prestación de servicios de salud al individuo [4]. HIPAA también establece estándares de privacidad para que las personas puedan entender y controlar como su información de salud es usada y su cumplimiento fue requerido a partir del 14 de abril del 2003.

La Regla de Seguridad. La cual establece normas nacionales para proteger la confidencialidad, integridad y disponibilidad de la información de salud protegida electrónica también conocidos como *electronic Protected Health Information* (ePHI) [4]. La regla tiene requerimientos y se hacen para que una entidad cubierta pueda ofrecer seguridad de la información de salud electrónica de los individuos. Las categorías de requerimientos son: procedimientos administrativos, salvaguardas físicas, servicios técnicos de seguridad y mecanismos técnicos. En la siguiente figura se explican las categorías [4].

Ilustración 3. Matriz de estándares de seguridad

Matriz estándares de seguridad – Apéndice A hasta subsección C de sección 164		
Estándares	Secciones	Especificaciones de implementación (R)=Requerido, (D)= Deseable
Salvaguardas Administrativas		
Proceso de gestión de la Seguridad	164.308(a)(1)	Análisis de Riesgos (R)
		Gestión del Riesgo (R)
		Política de Sanciones (R)
		Revisión de la Actividad del Sistema de Información (R)
Responsabilidad de seguridad asignada	164.308(a)(2)	(R)
Seguridad de la fuerza de trabajo	164.308(a)(3)	Autorización y/o Supervisión (D)
		Procedimiento de autorización de mano de obra (D)
		Procedimiento de Terminación (D)
Gestión de Acceso a la Información	164.308(a)(4)	Aislar las funciones del centro de atención de salud (R)
		Autorización de Acceso (D)
		Establecimiento de Acceso y modificación (D)
Concientización y Capacitación de Seguridad	164.308(a)(5)	Recordatorios de Seguridad (D)
		Protección contra Software Malicioso (D)
		Monitoreo de inicio de sesión (D)
		Gestión de claves (D)
Procedimientos de Incidentes de Seguridad	164.308(a)(6)	Reporte y Respuesta (R)
Plan de Contingencia	164.308(a)(7)	Plan de Respaldo de Datos (R)
		Plan de Recuperación de Desastres (R)
		Plan de Operación en modo Emergencia (R)
		Procedimiento de Revisión y Pruebas (D)
		Análisis de Datos Críticos y Aplicaciones (D)
Evaluación	164.308(a)(7)	(R)
Contratos de Socios de Negocios y Otros Arreglos	164.308(b)(2)	Contrato Escrito u otro Arreglo (R)
Salvaguardas Físicas		
Control de Acceso a Instalaciones	164.310(a)(1)	Operaciones de Contingencia (D)
		Plan de Segurida de la Instalación (D)
		Procedimientos de Control de Acceso y Validación (D)
		Registros de Mantenimiento (D)
Uso de la Estación de Trabajo	164.310(b)	(R)
Seguridad de la Estación de Trabajo	164.310(c)	(R)
Control de dispositivos y medios	164.310(d)(1)	Disposición (R)
		Reutilización de Medios (R)
		Trazabilidad (D)
		Almacenamiento y Respaldo de Datos (D)
Salvaguardas Técnicas		
Control de Acceso	§164.312(a)(1)	Identificador de usuario único (R)
		Procedimiento de acceso de emergencia (R)
		Desconexión automática (D)
		Cifrado y Descrifrado (A)
Controles de auditoria	§164.312(b)	(R)
Integridad	§164.312(c)(1)	Mecanismo para autenticar ePHI (A)
Autenticación de entidad o persona	§164.312(d)	(R)
Seguridad en la Transmisión	§164.312(e)(1)	Controles de Integridad (A)
		Cifrado (A)

Fuente: [4]

2.2.2 HITECH

La Health Information Technology for Economic and Clinical Health (HITECH) fue emitida en el 2009 y fortalece a la regla de Privacidad y Seguridad de HIPAA en su observación y penalidad en caso de incumplimiento [16]. La norma también reglamenta específicamente los datos de salud de las personas, pero aplica únicamente para los Estados Unidos de América. Los puntos más notables de la ley son:

- Notificaciones por parte de las entidades cubiertas y los socios de negocios ante incidentes de seguridad con la PHI al departamento de salud y servicios humanos. Además, se debe notificar a los individuos o titulares de la PHI.
- Creación de cuatro categorías de violaciones que reflejan los niveles de culpabilidad. Así mismo, cuatro niveles de penalización por cada categoría de infracción, tal como se muestra en la figura abajo.

Ilustración 4. Categorías de infracciones y montos respectivos de penalidad

Categoría de infracción Section 1176(a)(1) HITECH	Cada Infracción	Todas las violaciones de una disposición idéntica en un año calendario
(A)No sabia….....	$100 - $50,000	$1,500,000
(B)Causa razonable ….....	1,000 - 50,000	1,500,000
(C)(i) Negligencia intencional – Corregida….....	10,000 - 50,000	1,500,000
(C)(ii) Negligencia intencional – No Corregida ….....	50,000	1,500,000

Fuente: Elaboración propia

2.2.3 Reglamento General de Protección de Datos 2016/679 Unión Europea

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece un marco sólido y coherente en materia protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. Así también, se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Se debe notar que el RGPD aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea,

independientemente de que el tratamiento tenga lugar en la Unión o no, en consecuencia, no es una ley centrada en un país sino en los derechos de sus residentes como tal [17].

El RGPD define como “datos relativos a la salud” como “a los datos personales relativos a la salud física y mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud” [17] y son tratados como una categoría especial de acuerdo al artículo 9 apartado 1 [17]. Solo se pueden tratar estos datos bajos las siguientes excepciones:

- El interesado da su consentimiento explícito para el tratamiento de dichos datos personales.
- Es necesario para proteger intereses vitales del interesado o de otra persona física, siempre y cuando el interesado no esté capacitado física o jurídicamente para dar su consentimiento.
- Es necesario para fines de medicina laboral o preventiva, evaluación del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario, y gestión de sistemas y servicios de asistencia sanitaria y social.
- En el ámbito de salud pública por razones de salud pública como la protección frente a amenazas transfronterizas graves para la salud.

El RGPD define para el tratamiento de los datos personales los siguientes principios:

- Licitud, lealtad y transparencia. El interesado da su consentimiento para el tratamiento de sus datos de manera lícita, leal y transparente.
- Minimización de datos. Adecuados, pertinentes y limitados en relación con los fines de tratamiento.
- Exactitud. Datos exactos y de ser necesario actualizados o rectificados.
- Limitación del plazo de conservación.

- Integridad y confidencialidad. Garantizar la seguridad adecuada de los datos personales, protección contra el tratamiento no autorizado, contra pérdida, destrucción o daño accidental, mediante el uso de medidas técnicas u organizativas apropiadas.
- Responsabilidad proactiva. El responsable del tratamiento de datos será el encargado de dar cumplimiento al reglamento y capaz de demostrarlo.

2.2.4 Análisis de las leyes

Primero, HIPAA es una ley creada específicamente para regular, estandarizar y asegurar la privacidad de la información de salud identificable individualmente, mientras que RPGD sirve para proteger el tratamiento y la libre circulación de los datos personales de los residentes físicos de la Unión Europea.

Segundo, se debe notar que HIPAA es una ley centrada en las organizaciones y su cobertura geográfica solo aplica a proveedores de salud, consumidores y sistemas dentro de los Estados Unidos de América. Mientras que RPGD es una ley centrada en el consumidor por lo cual aplica a cualquier organización en el mundo que requiera tratar datos de usuarios de la Unión Europea. En conclusión, el HIPAA tiene más afinidad con la seguridad de la HCE por tanto usaremos su marco de referencia para nuestro diseño, aplicando algunos criterios generales de RPGD cuando sea necesario.

Tercero, HIPAA consta de una “Regla de Privacidad” que protege la PHI que es información electrónica, oral y escrita. Y una “Regla de Seguridad” que aplica únicamente a la ePHI, por tanto, nos centraremos en la Regla de Seguridad para diseñar nuestra solución.

Siguiendo con la línea en HIPAA podemos obtener los tres puntos esenciales de la seguridad de la información:

- Confidencialidad. La ePHI es accesible sólo por las personas y procesos autorizados.

- Integridad. La ePHI no se modifica ni se destruye de manera no autorizada.
- Disponibilidad. La ePHI siempre está disponible para ser revisada por las personas y procesos autorizados.

3. Estado actual del tema

En el 2015 Zyskind, Nathan y Pentland [18] publicaron un trabajo para el uso de cadenas de bloques para la protección de datos personales, centrando sus esfuerzos en la protección de los datos que usan las aplicaciones de los móviles. En agosto del 2016 un grupo del MIT y del Beth Israel Deaconess Medical Center [19] también publicó un trabajo del uso de la cadena de bloques en el campo de cuidados de salud, donde proponen el sistema MedRec que gestiona la autenticación, confidencialidad, logs y el intercambio de datos, las cuales son consideraciones cruciales al manejar información sensible.

El 6 de julio del 2016 la ONC [20] anunció el reto "Uso de la Cadena de Bloques en la salud IT y la investigación relacionada con la salud", donde se solicitó examinar cómo el uso de la Cadena de Bloques podía promover las necesidades de interoperabilidad de la industria expresadas en el *Shared Nationwide Interoperability Roadmap* [21] del ONC. La ONC recibió 70 propuestas del público, de las cuales se seleccionaron 15 opciones ganadoras en agosto 29 del 2016 [20].

El reporte realizado por Culver "*Blockchain Technologies: A discussion on how the claims process can be improved*" [20] entrega una solución basada en contratos inteligentes para agilizar el proceso de costeo de la atención sanitaria, construyendo una plataforma interoperable, transparente y exacta. De esta manera, ahorra tiempo y esfuerzo en el proceso de reclamaciones actual ante los seguros de salud. La solución contempla codificar en un contrato inteligente la relación entre los proveedores de salud, los pacientes y los seguros médicos, de tal forma que en la cadena de bloques solo se almacene una *Uniform Resource Locator* (URL para disminuir la cantidad de datos que almacena la cadena y mantiene la privacidad del paciente integrando un hash con datos propios [4]

En 2017 Xia y otros presentaron MedShare [22] que se trata de un sistema Blockchain seguro para el intercambio de datos médicos entre grandes custodios en un entorno no confiable, proporcionando no repudio, auditoría y control. Su diseño emplea contratos inteligentes y un mecanismo de control de acceso para realizar un seguimiento efectivo al comportamiento de los datos. De tal forma, que si se detecta una violación de permisos se deniega el acceso a la entidad infractora.

En julio del 2017 Roehrs y otros publicaron OmniPHR [23] el cual es un modelo de arquitectura distribuida para integrar registros de salud personales. La propuesta permite una vista unificada, integrando los registros de salud dispersos de los pacientes. OmniPHR promueve la interoperabilidad entre diferentes proveedores para acceder al registro de salud.

En 2018 Zhang y otros presentaron FHIRCHAIN [24] que es un prototipo diseñado sobre *Ethereum Blockchain* para compartir datos clínicos de forma segura y escalable. El diseño de FHIRChain aborda cinco requisitos clave proporcionados por la ruta de interoperabilidad de la ONC [20] e incluye: la identificación y autenticación del usuario, el intercambio seguro de datos, el acceso de datos autorizado, los formatos de datos consistentes y la modularidad del sistema.

El 31 de agosto del 2019 Hales y Zeng publicaron HealthChain [25] que se trata de un marco de trabajo usando *Hyperledger Blockchain* para el intercambio de registros de salud centrados en el paciente. intenta reforzar la participación del paciente, la conservación de datos y la difusión regulada de la información en un entorno seguro e interoperable.

En octubre del 2019 Heinrich y otros [26] publican “Hacia una arquitectura basada en blockchain para los registros electrónicos de salud orientada a los interesados : estudio de investigación de ciencia del diseño”, que tuvo como objetivo introducir la tecnología blockchain para los EHR, basado en la identificación de las partes interesadas y obtener sistemáticamente sus requisitos. Y concluye discutiendo los beneficios clave y los desafíos clave de la tecnología blockchain en el contexto de los EHR.

4. Fundamentos para la selección de la Cadena de Bloques Hyperledger

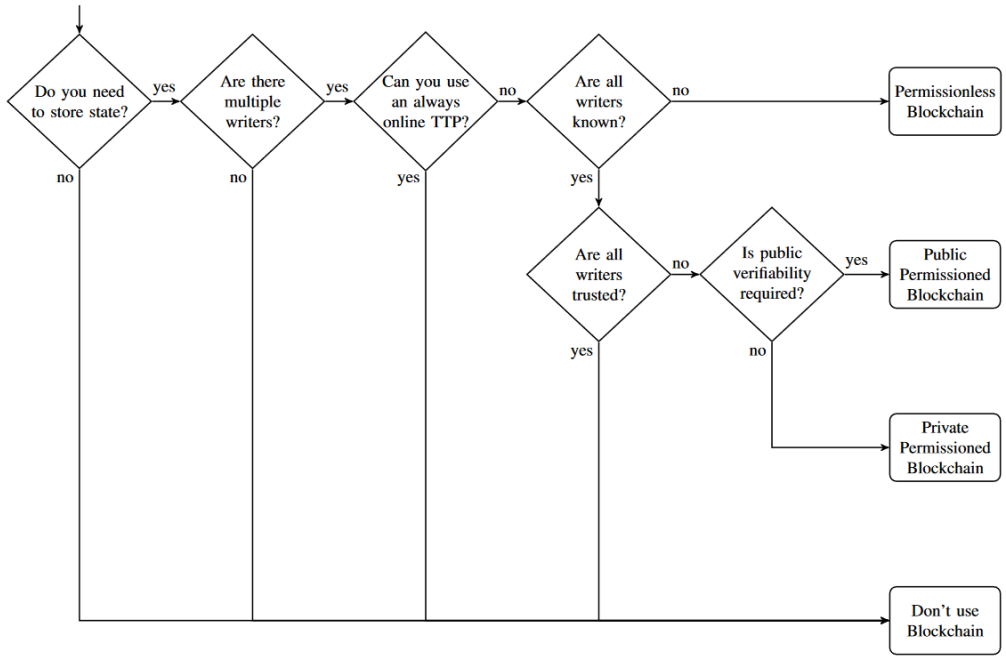
4.1 Modelos de decisión para la cadena de bloques

Existen algunos modelos que sustentan el uso de una cadena de bloques. Todos se centran en dos preguntas principales: ¿necesidad de ente central de confianza?, ¿miembros no confiables?, por lo tanto, se revisarán a continuación algunos modelos de selección.

4.1.1 Modelo de Wüst y Gerbais [27].

Este modelo proporciona una metodología estructurada para determinar la solución técnica adecuada para resolver un problema de aplicación particular. El diagrama de flujo de la ilustración inferior determina cuando una cadena de bloques es una solución técnica adecuada, para nuestro caso analizaremos paso a paso:

Ilustración 5. Modelo de decisión de Wüst y Gerbais



Fuente: [27]

- ¿Se necesita guardar un estado? Si, se necesita guardar los estados o modificaciones que sufre la HCE en un orden cronológico inmutable.
- ¿Hay múltiples escritores? Si existen múltiples escritores que pueden modificar la HCE. Dado que una HCE es una recopilación

aportada por varios actores como casas de salud, profesionales de salud y hasta aplicativos o dispositivos de salud.

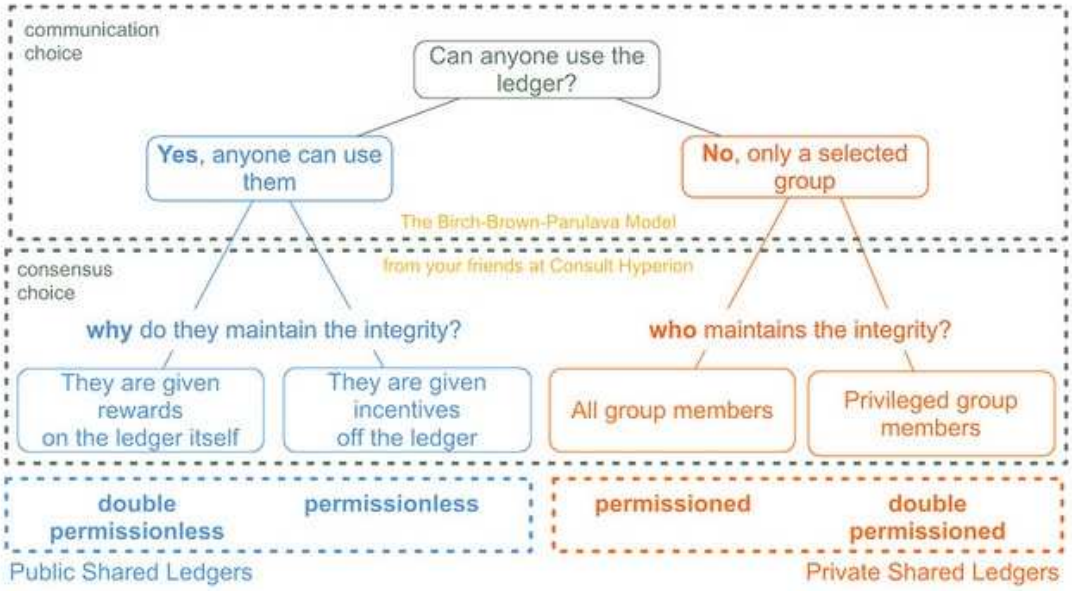
- ¿Puedes usar siempre un tercero confiable en línea? No existe un ente central en línea que regule las modificaciones sobre una HCE. Al tener múltiples orígenes y no existir un ente central de confianza que valide los cambios se necesita un mecanismo de consenso o aprobación de cambios o nuevos registros añadidos a la HCE.
- ¿Todos los escritores de HCE son conocidos? Si todos los que pueden modificar la HCE son conocidos y son proveedores de salud.
- ¿Los escritores de HCE son de confianza? No, todos los escritores no son de confianza porque entran especialistas, centros de salud, aplicaciones de salud en dispositivos móviles, etc.
- ¿Se necesita verificación pública de los datos? No se necesita que todo el mundo pueda entrar a verificar la información contenida en la cadena de bloques, pero si es necesario que los usuarios puedan verificar la integridad de la cadena.

Se puede concluir en base al flujo analizado que requerimos una solución del tipo: Cadena de bloques privada autorizada en base al modelo Wüst y Gerbais.

4.1.2 Modelo de Birch-Brown-Parulava [28]

Este modelo no ayuda a decidir si la cadena de bloques es la tecnología idónea, pero ayuda a decidir qué tipo de cadena se debe implementar:

Ilustración 6 Modelo Birch-Brown-Parulava



Fuente: [28]

Se navegará por el árbol de decisión para llegar a una conclusión:

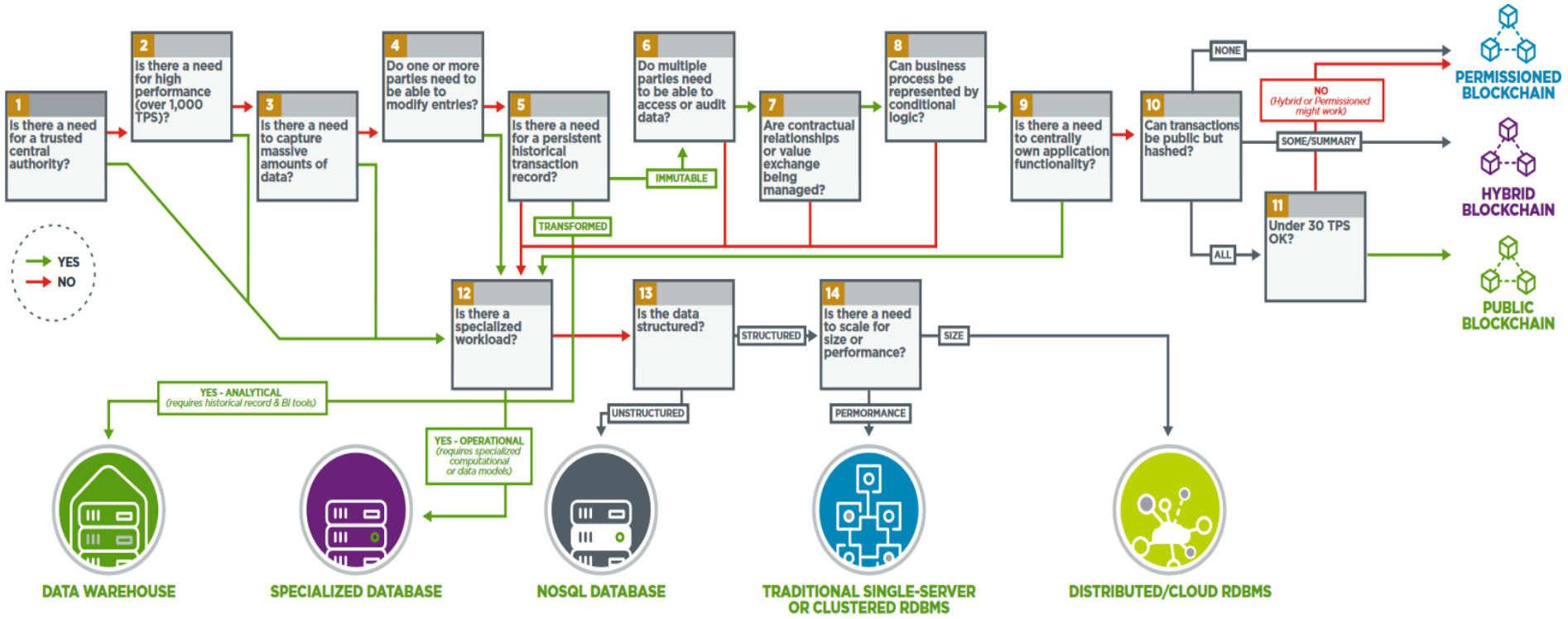
- ¿Cualquier puede usar la cadena de bloques? Para nuestro caso solo un grupo de miembros se le permitirá acceder a la cadena de bloques con permisos de lectura-escritura. Pero aquí se realiza una doble elección porque todos los habitantes deben poder participar en la cadena, pero siendo gestionados por una entidad central que asigne identidades y permisos.
- ¿Quién mantiene la integridad de la cadena de bloques? Únicamente un grupo privilegiado de miembros, considerando nuestro caso deben ser los hospitales públicos y entidades como el ministerio de salud los únicos que puedan llegar al consenso.

Como conclusión el modelo de Birch-Brown-Parulava nos conduce a una cadena del tipo privada con autorización.

4.1.3 Modelo Árbol de decisión de CompTIA [29]

El consejo de asesoría Blockchain de COMPTIA creo un árbol visual de decisión y una infografía práctica para guiar a los usuarios a través de una serie de caminos que le ayudan a decidir si la Cadena de Bloques u otra solución es la más idónea.

Ilustración 7 CompTIA Blockchain Decision Tree



Fuente: [29]

Para recorrer el camino se deben realizar 11 preguntas:

- ¿Hay la necesidad de una entidad central de confianza? No, en nuestro caso existen varios actores que interactúan con la red de salud.
- ¿Hay necesidad de alto rendimiento (más de 1,000 transacciones por segundo)? No, en nuestro caso los EHR se almacenan *off the chain o* fuera de la cadena. Además, así un ente de salud genere 1000 registros por una atención solo se irá a la cadena de bloques un solo puntero por la atención completa.
- ¿Existe la necesidad de captar cantidades masivas de datos? No, como se indicó los datos del paciente serán almacenados fuera de la cadena por lo cual no se subirán datos masivos.
- ¿Una o más partes pueden modificar la entrada? No, se debe observar que los EHR deben tener integridad por lo tanto no se deberían modificar una vez que el hash del puntero es subido a la cadena de bloques. Pero, desde el punto de vista teórico la Cadena de bloques no permite la modificación de un registro en un bloque. Sin embargo, desde el punto de vista práctico si deseamos realizar una modificación sobre los EHR de un paciente, esto se debe traducir en una entrada de ajuste para crear el efecto “modificación”.
- ¿Existe la necesidad de un registro histórico persistente de transacciones? Si, para tener una HCE completa se debe tener todos los registros inmutables y ordenados históricamente.
- ¿Muchas partes deben poder acceder o auditar los datos? Si, la HCE se debe poder acceder por los distintos proveedores de salud.
- ¿Se manejan relaciones contractuales o cambios de valor? Si, se deben manejar como contratos los permisos que se otorgan a entes de salud para que accedan a los EHR que residen en otro proveedor de salud. Por tanto, los valores o variables del contrato pueden cambiar ya que se pueden adicionar o eliminar permisos de acceso más no las transacciones o registros de salud.

- ¿El proceso del negocio se puede representar con lógica condicional? Si, se debe programar varios contratos usando lógica condicional para representar la administración de una HCE.
- ¿Existe la necesidad de una aplicación central propia? No, los pacientes y proveedores de saluda deben tener la capacidad de ejecutar sus propias aplicaciones que validen o auditen ciertas variables del contrato y el registro de transacciones. Por ejemplo, un aplicativo de salud corriendo en un reloj que mide pulsaciones, presión temperatura, debería con el permiso del usuario poder subir punteros con la información que recolecta fuera de la Cadena de bloques.
- ¿Las transacciones deben ser públicas, pero ofrecidas en modo hash? Este punto es intermedio, como el sistema debe manejar las HCE de los habitantes del Ecuador evidentemente deben ser públicas en formato resumen o Hash, pero dentro de un ambiente controlado que solo permita la lectura, pero no la escritura desde cualquier nodo. Todo esto controlado desde un contrato inteligente.

De acuerdo con lo analizado el resultado sería una Cadena de bloques autorizada o una cadena de bloques hibrida (autorizada + no autorizada).

4.1.4 Análisis final de los modelos de selección

Si bien no se citan todos los modelos, solo se tomaron los 3 principales y usando la navegación a través de los modelos podemos concluir que se puede usar como solución para el mantenimiento de las HCE una Cadena de bloques del tipo Autorizada. Ya que cumple con los siguientes criterios:

- Los participantes deben ser identificados o identificables.
- Las redes necesitan ser autorizadas.
- Alta tasa de rendimiento de transacciones o tiempo de asentamiento del bloque.
- Baja latencia de confirmación de transacción debido al consenso delegado a un grupo de nodos conocidos.

- Privacidad y confidencialidad de transacciones y datos relacionados con transacciones comerciales.

4.2 Tipo de cadena de bloques: Privada, Pública o hibrida en cumplimiento con HIPAA

La literatura actual categoriza la Cadena de Bloques de acuerdo con su administración y permisos en tres tipos: Pública, Privada o Federada.

En una Cadena de Bloques Pública se puede unir cualquier usuario y convertirse en un nodo usuario o nodo minero, se podría decir que es una red sin permisos. Además, todos los participantes pueden realizar transacciones o contratos. Por último, cualquier nodo puede formar parte del algoritmo de consenso.

La Cadena de Bloques Privada pertenece a una categoría de Cadena de Bloques llamadas “Autorizadas” donde se define una lista blanca de usuarios permitidos con características y permisos particulares sobre las operaciones de red [3]. Esto cumple con el primer punto de las Salvaguardas técnicas de HIPAA para control de acceso tal como muestra la figura abajo.

Tabla 1. Cumplimiento con HIPAA - Salvaguardas Técnicas - Control de Acceso 1

Control de acceso		
Especificación de la norma	Descripción HIPAA	Cadena de bloques
Identificación única de usuario (Requerida)	La Identificación única de usuario permite a una entidad realizar un seguimiento de la actividad específica de cada usuario cuando está conectado a un sistema de información. Así, se pueden asignar responsabilidades de las funciones que se realizan en los sistemas de información con ePHI cuando los usuarios se conectan a dichos sistemas. §164.312(a)(1)	Esto es configurable en Cadenas de Bloques Privadas o Federadas. Para tener la granularidad necesaria se pueden establecer atributos de contratos inteligentes que solo se logra con la implementación de Hyperledger.

Fuente: Elaboración propia.

La Cadena de Bloques tiene varias limitaciones y debilidades, aún la privacidad y confidencialidad siguen siendo un problema porque la información se almacena dentro de los nodos de la red de modo público. Se

pueden adoptar varios mecanismos de anonimizar datos o cifrado para proteger la confidencialidad de la información [3]. La naturaleza de los contratos inteligentes hace que su operación sea difícil de entender o tengan comportamientos ilegales o extraños [30]. Otro problema asociado de almacenar datos en la Cadena de Bloques es la escalabilidad, todo almacenamiento de datos o modificación dentro de un contrato inteligente o una transacción se distribuyen como una copia completa a todos los nodos de la Cadena de Bloques, sin contar con los honorarios que se debe pagar por la ejecución o llamada de un contrato o transacción [24].

Por tal motivo, en lugar de almacenar los datos de salud cifrados en la cadena de bloques vamos a almacenar metadatos cifrados que hagan referencia a la información protegida. De tal manera, que el intercambio de punteros cifrados permite conservar la propiedad de los datos en los proveedores y resolver el problema de escalabilidad. Basándonos en estas consideraciones podemos ver en la tabla de abajo como se afecta el cumplimiento del HIPAA.

Tabla 2 Cumplimiento con HIPAA - Salvaguardas Técnicas - Control de Acceso 1

Control de acceso		
Especificación de la norma	Descripción HIPAA	Cadena de bloques
Procedimiento de acceso de emergencia (Requerida)	El procedimiento de acceso de emergencia son instrucciones documentadas y prácticas operativas para obtener acceso a la ePHI necesaria durante una situación de emergencia. Los controles de acceso son necesarios en condiciones de emergencia, aunque pueden ser muy diferentes de los utilizados en circunstancias de operación normal. §164.312(a)(1)	El procedimiento de acceso de emergencia queda para cumplimiento de cada proveedor de salud y no forma parte de la cadena de bloques, debido a que la cadena no contiene los datos, sino que contiene referencias cifradas hacia los datos.

Desconexión automática (Deseable)	La desconexión automática es una forma efectiva de impedir que usuarios no autorizados accedan a ePHI en una estación de trabajo cuando se deja sin atención durante un período de tiempo. Después de un período predeterminado de inactividad, la aplicación automáticamente desconectará al usuario.	Desde el punto de vista de un usuario del sistema de salud, es una funcionalidad sencilla de implementar y no compete a la tecnología Cadena de Bloques, es una funcionalidad de la "billetera" o aplicación del usuario. En cuanto al punto de vista del proveedor de salud debe ser implementado en sus sistemas informáticos propios.
Cifrado y descifrado (Deseable)	Si la información está cifrada, habría una baja probabilidad de que cualquier persona que no sea la parte receptora sea capaz de descifrar el texto. El objetivo del cifrado es proteger a EPHI de ser accedida por usuarios no autorizados.	Los punteros contenidos en la Cadena de Bloques estarán cifrados y serán descifrables solo por los usuarios autorizados usando la infraestructura de clave pública [31].

Fuente: Elaboración propia.

Para los dos controles de seguridad adicionales de transmisión de la información presentamos la siguiente tabla.

Tabla 3. Cumplimiento con HIPAA - Salvaguardas Técnicas – Seguridad de la Transmisión

Seguridad en la transmisión		
Especificación de la norma	Descripción	Cadena de bloques
Controles de Integridad (Deseable)	Implementar medidas de seguridad para asegurar que la ePHI transmitida sobre una red de telecomunicaciones no se modifique indebidamente sin detección hasta que sea entregada a su receptor.	El control de integridad es parte del comportamiento por defecto de la Cadena de Bloques utilizando hashing [31].
Cifrado (Deseable)	Implementar un mecanismo para cifrar ePHI cuando se transmite a sobre una red de telecomunicaciones.	Se indicó que la Cadena de Bloques va a contener punteros por temas de escalabilidad, por lo cual

		el cifrado para la transmisión de datos se debe realizar entre el emisor y receptor usando alguna técnica conocido de cifrado [31].

Fuente: Elaboración propia.

Se puede evidenciar que la solución de la Cadena de Bloques nos va direccionando únicamente al control de la HCE y no al manejo total de los datos por todos los temas ya revisados. Por tanto, en el siguiente capítulo se realizará el diseño enfocado en el tema de permisos de acceso y transferencia.

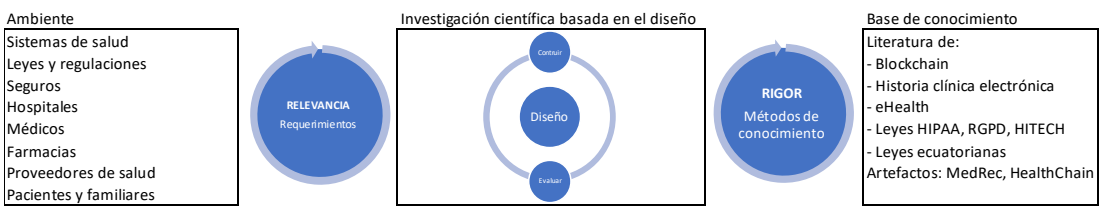
5. Diseño y arquitectura de la solución sobre la cadena de bloques Hyperledger

5.1 Grupo de interesados de la HCE para el diseño

Nuestra tesis se apoyará en el trabajo de Heinrich [26] donde introduce la tecnología *blockchain* para EHR, basada en la identificación de partes interesadas donde sistemáticamente obtiene los requisitos, discutiendo los beneficios clave y los desafíos de la tecnología *blockchain* en el contexto de la HCE.

El desarrollo de una solución es influenciado por su entorno y el cuerpo de conocimiento existente como podemos ver en la figura abajo [32]. Hemos adaptado los tres ciclos de Hevner [32] para las historias clínicas electrónicas. En el ciclo de relevancia toma requerimientos del ambiente dentro de la investigación. El ciclo de rigor proporciona teorías y la experiencia de la base de conocimientos en la investigación y agrega cualquier nuevo conocimiento generado a la base. El ciclo de diseño construye y evalúa artefactos – procesos de diseño en la actividad de investigación [33].

Ilustración 8 Método de la investigación científica basada en el diseño para HCE



Fuente: Elaboración propia, adaptación de Hevner [32]

Heinrich [26] uso el método de investigación basado en el diseño para encontrar y separar los grupos de interesados en tres clasificaciones como se muestra en la figura abajo. Los interesados primarios son los directamente involucrados en la prestación del cuidado médico, los secundarios son entes ligados al paciente a través de algún convenio o grado familiar. Además, los terciarios que no tienen una relación directa con el cliente, pero si con los EHR.

Ilustración 9 Interesados en los EHR

Registros de Salud Electrónicos		
Interesados Primarios	**Interesados Secundarios**	**Interesados Terciarios**
Médicos	Seguros	Sociedad
Pacientes	Familiares y parientes	Institutos de investigación
Cuidadores y enfermeras	Empleadores	Autoridades públicas
Terapeutas		Industrias de salud
Farmacéuticos		
Clínicas y hospitales		
Laboratorios		
Hogares de ancianos		

Fuente: Elaboración adaptada de Heinrich [26]

5.2 Requisitos de la HCE para el diseño

Saquero [34] en el 2011 establece los requisitos que debe satisfacer una HCE y son: autenticación, autorización, integridad, no repudio, confidencialidad y consentimiento.

Rodrigues [35] en el 2013 también establece requisitos para asegurar la seguridad y privacidad de las HCE: Acceso autorizado, confidencialidad, consentimiento del paciente, propiedad de la información, consistencia de la información, auditable y almacenamiento de la información como se describe en la tabla abajo.

Tabla 4. Requerimientos de la HCE

Requerimientos	Descripción

Acceso autorizado	Se debe implementar un sistema de identificación para pacientes y proveedores de atención médica. Esta identificación debe ser portable entre las diferentes entidades que tienen acceso a los datos de los pacientes. Este sistema puede lograrse mediante la identificación de cada paciente. En cuanto a la autenticación, un sistema centralizado basado en una clave pública es viable. Se debe implementar un control de acceso basado en roles o RBAC para permitir que el personal autorizado acceda a ciertos datos en función de su rol.
Confidencialidad	Para garantizar la confidencialidad del proceso de comunicación, se utilizan algoritmos de cifrado. Sin embargo, el problema de confidencialidad en un sistema distribuido surge porque no es posible que el sistema transmisor de información verifique que la confidencialidad no ha sido expuesta en el extremo receptor.
Consentimiento del paciente	De acuerdo con la legislación, los pacientes deben permitir o negar el acceso a su información clínica. Este consentimiento puede ser implícito o explícito. Otro hecho a considerar es la necesidad de obtener acceso a la HCE en la entidad alojada desde otra entidad externa para lo cual se debe contar con el consentimiento del paciente, pero en caso de emergencia, se debe proporcionar un mecanismo de seguridad para evitar esta restricción sin el consentimiento del paciente.
Propiedad de la información	La propiedad de la HCE no está claramente establecida. El personal médico es responsable de esta información. Sin embargo, los propios pacientes tienen derecho a acceder a su información clínica.
Consistencia de la información	En un esquema de interoperabilidad, se debe crear un mecanismo de notificación para mostrar los cambios en la información. Este sistema debe permitir el acceso a las versiones anteriores de los EHR, si es necesario.
Auditorias	Un registro de auditoría debe incluir todos los accesos a la información y todos los cambios que han tenido lugar en los EHR. Este sistema permite monitorear el acceso y es una herramienta poderosa para garantizar un sistema seguro.

Almacenamiento	Los registros médicos deben almacenarse por un período de tiempo establecido, de acuerdo con la legislación del país respectivo. Después de este período de tiempo, los datos médicos pueden ser eliminados. Sin embargo, esto no se recomienda cuando se trata de la gestión y práctica de EHR, donde el objetivo es mantener la información médica completa sobre el paciente durante toda su vida.

Fuente: Elaboración propia adaptada de Rodrigues [35]

Heinrich [26] establece requisitos para le HCE usando un grupo de 9 expertos obtenidos en el grupo de interesados primarios obteniendo 27 requisitos. Los requisitos que son parte de la seguridad informática son: seguridad, privacidad, control de acceso/permisos, confirmación de identidad, integridad, modo verificación y acceso de emergencia. Por último, los otros requerimientos son temas básicos de la ingeniería de software tal como se muestra en la ilustración de abajo:

Ilustración 10 Requisitos de interesados basado en el método de investigación científica basada en el diseño [32]

	Requisito
Interesados primarios	Seguridad de los datos
	Privacidad de los datos
	Control de Acceso/Permiso, soberania de datos
	Confirmación de identidad
	Protección contra manipulación/Integridad de datos
	Registro completo de salud
	Rendimiento
	Diseño amistoso con el usuario
	Información especifica de contexto
	Almacenamiento de datos
	Compartición de datos
	Estandar consistente y operable
	Comunicación intersectorial
	Garantizar relaciones de confianza
	Derechos de creación, lectura, actualización y borrado.
	Modo verificación
	Acceso de emergencia
	Medicación/Plan de salud
	Seguimiento de las transiciones de estado
	Asuntos administrativos generales
	Sincronización fuera de la cadena
	Servicios de notificación
	Modularidad
	Centrado al paciente
	Soporte de flujo de trabajo
	Integración con los sistemas existentes
	Hoja de transferencia

Fuente: Elaboración propia adaptada de Heinrich [26]

La regla de seguridad de HIPAA [36] por otro lado define salvaguardas administrativas: Proceso de gestión de la seguridad, oficial de seguridad, gestión de acceso a la información, capacitación-gestión de la fuerza laboral y evaluación. También define salvaguardas físicas que se pueden posicionar como requisitos: control y acceso a las instalaciones, seguridad en la estación de trabajo y el dispositivo. Por último, define salvaguardas técnicas que

podemos tomar como requisitos: control de acceso, controles de auditoria, controles de integridad y seguridad en la transmisión.

Tabla 5. Matriz de requisitos HIPAA Security Rule

Matriz estándares de seguridad – Apéndice A hasta subsección C de sección 164		
Estándares	Secciones	Especificaciones de implementación (R)=Requerido, (D)= Deseable
Salvaguardas Administrativas		
Proceso de gestión de la Seguridad	164.308(a)(1)	Análisis de Riesgos (R) Gestión del Riesgo (R) Política de Sanciones (R) Revisión de la Actividad del Sistema de Información (R)
Responsabilidad de seguridad asignada	164.308(a)(2)	(R)
Seguridad de la fuerza de trabajo	164.308(a)(3)	Autorización y/o Supervisión (D) Procedimiento de autorización de mano de obra (D) Procedimiento de Terminación (D)
Gestión de Acceso a la Información	164.308(a)(4)	Aislar las funciones del centro de atención de salud (R) Autorización de Acceso (D) Establecimiento de Acceso y modificación (D)
Concientización y Capacitación de Seguridad	164.308(a)(5)	Recordatorios de Seguridad (D) Protección contra Software Malicioso (D) Monitoreo de inicio de sesión (D) Gestión de claves (D)
Procedimientos de Incidentes de Seguridad	164.308(a)(6)	Reporte y Respuesta (R)
Plan de Contingencia	164.308(a)(7)	Plan de Respaldo de Datos (R) Plan de Recuperación de Desastres (R) Plan de Operación en modo Emergencia (R) Procedimiento de Revisión y Pruebas (D) Análisis de Datos Críticos y Aplicaciones (D)
Evaluación	164.308(a)(7)	(R)
Contratos de Socios de Negocios y Otros Arreglos	164.308(b)(2)	Contrato Escrito u otro Arreglo (R)
Salvaguardas Físicas		
Control de Acceso a Instalaciones	164.310(a)(1)	Operaciones de Contingencia (D) Plan de Seguridad de la Instalación (D) Procedimientos de Control de Acceso y Validación (D)

		Registros de Mantenimiento (D)
Uso de la Estación de Trabajo	164.310(b)	(R)
Seguridad de la Estación de Trabajo	164.310(c)	(R)
Control de dispositivos y medios	164.310(d)(1)	Disposición (R) Reutilización de Medios (R) Trazabilidad (D) Almacenamiento y Respaldo de Datos (D)
Salvaguardas Técnicas		
Control de Acceso	§164.312(a)(1)	Identificador de usuario único (R) Procedimiento de acceso de emergencia (R) Desconexión automática (D) Cifrado y Descifrado (D)
Controles de auditoria	§164.312(b)	(R)
Integridad	§164.312(c)(1)	Mecanismo para autenticar ePHI (D)
Autenticación de entidad o persona	§164.312(d)	(R)
Seguridad en la Transmisión	§164.312(e)(1)	Controles de Integridad (D) Cifrado (D)

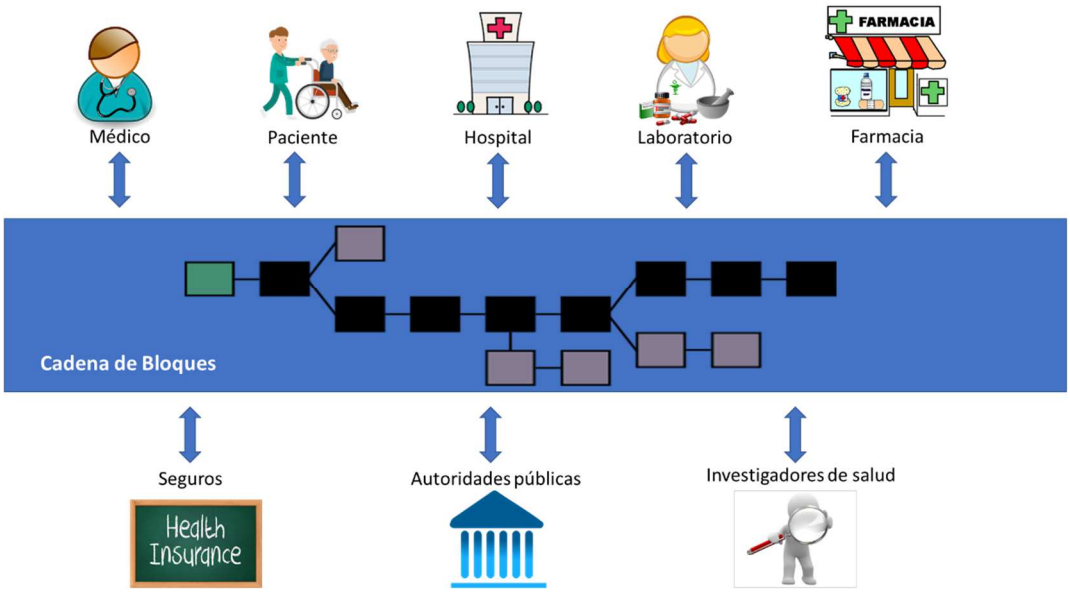
Fuente: [4]

5.3 Arquitectura de la solución para HCE usando Cadena de bloques.

5.3.1 Mapa conceptual de la solución

Como primera iteración se desarrolló un modelo basado en los requerimientos revisados en la sección 5.2, más los grupos de interesados de la sección 5.1 y los modelos de selección analizados en la sección 4.4.1. dando como resultado el primer mapa conceptual de la solución que se muestra abajo.

Ilustración 11 Mapa conceptual de una solución para el control de HCE



Fuente: Elaboración propia

En el mapa conceptual se muestra sobre la parte superior todos los entes primarios que interactúan con la Cadena de Bloques directamente con datos del paciente. En la parte inferior los actores que interactúan de forma directa con la cadena de bloques, pero indirectamente con los datos del paciente. En orden se describirán las interacciones descubiertas por cada actor en base a entrevistas realizadas a tres doctores con más de diez años de experiencia en Ecuador:

- Médico. Posee las siguientes interacciones con la cadena de bloques en orden de eventos
    - Solicitud de autorización para revisión de la HCE del paciente. Es una solicitud realizada por el médico tratante para poder con su identificación acceder a la información del paciente con permisos de lectura y escritura.
    - Lectura de datos de salud de la HCE del paciente. Interacción con la cadena de bloques que le permite al médico recuperar la totalidad de registros del usuario.
    - Escritura de datos de salud sobre la HCE del paciente. Interacción con la cadena de bloques que le permite al

médico escribir datos vitales, nuevos diagnósticos, prescripciones médicas y nuevas citas para consultas.

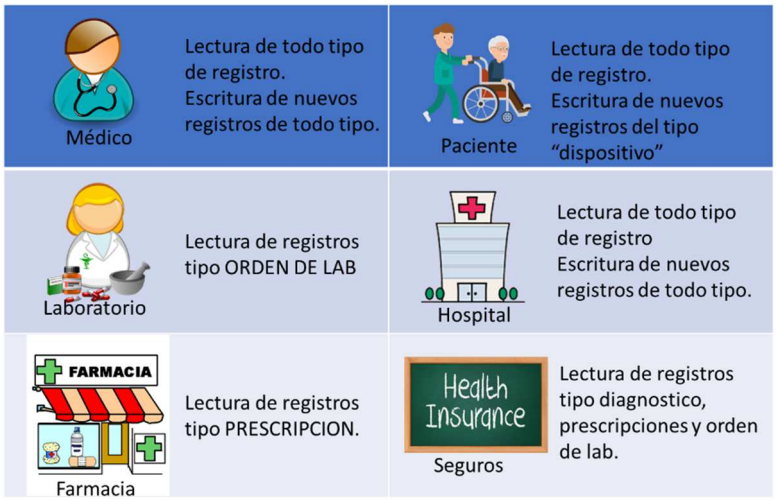
- Paciente. El paciente al ser el dueño y poseer accesos sobre su HCE puede realizar las siguientes interacciones:
    - Aceptación o rechazo de autorizaciones para lectura y escritura de su HCE. Interacción con la Cadena de bloques que permite a los médicos, hospitales, centros de salud, farmacias puedan leer y escribir nuevos registros de salud.
    - Lectura de nuevos registros de salud añadidos a su HCE. Interacción con la Cadena de Bloques que habilita la recuperación y lectura de cualquier nuevo registro de salud añadido a su HCE.
    - Autorización para que dispositivos puedan escribir sobre su HCE. Debido a los dispositivos electrónicos que apoyan la salud como relojes medidores de datos vitales, aplicaciones para medir el sueño esta interacción permite autorizar la escritura de datos sobre la HCE del paciente.
- Hospital.
    - Solicitud de autorización para revisión de la HCE del paciente. Interacción que emite solicitud al paciente para que un hospital, clínica o centro de salud pueda acceder a sus datos.
    - Lectura de datos de salud de la HCE del paciente. Esta interacción con la cadena de bloques permite al hospital recuperar todos los registros de un paciente.
    - Escritura de datos de salud sobre la HCE del paciente. Esta interacción con la cadena de bloques permite al hospital escribir sobre la HCE de un paciente.
- Laboratorio.
    - Lectura de datos de salud de la HCE del paciente. Interacción que permite leer la orden de exámenes a los cuales el paciente debe ser sometido.

    - Escritura de datos de salud sobre la HCE del paciente. La interacción permite escribir los resultados de laboratorio sobre la HCE de un paciente.
- Farmacia
    - Lectura de datos de salud de la HCE del paciente. Esta interacción permite leer las prescripciones o recetas que han sido enviadas para el paciente.
    - Escritura de datos sobre la HCE del paciente. Permite escribir un registro de la medicación entregada al paciente.
- Seguros de salud
    - Lectura de datos de salud de la HCE del paciente. Esta interacción le permite al seguro leer diagnósticos, prescripciones, resultados de laboratorio para poder realizar sus operaciones de pagos.
- Autoridades de salud e investigadores médicos.
    - Interactúan con las cadenas de bloques en modo lectura para buscar datos anonimizados sobre diagnósticos para la ayuda de estadísticas e investigaciones.

5.3.2 Consideraciones de diseño de la solución

En este punto ya podemos indicar que se necesita un control de acceso basado en roles o RBAC [37] para poder segregar las partes de información a las que puede acceder cada interesado sobre la información contenida en la cadena de bloques [34] tal como muestra la figura abajo.

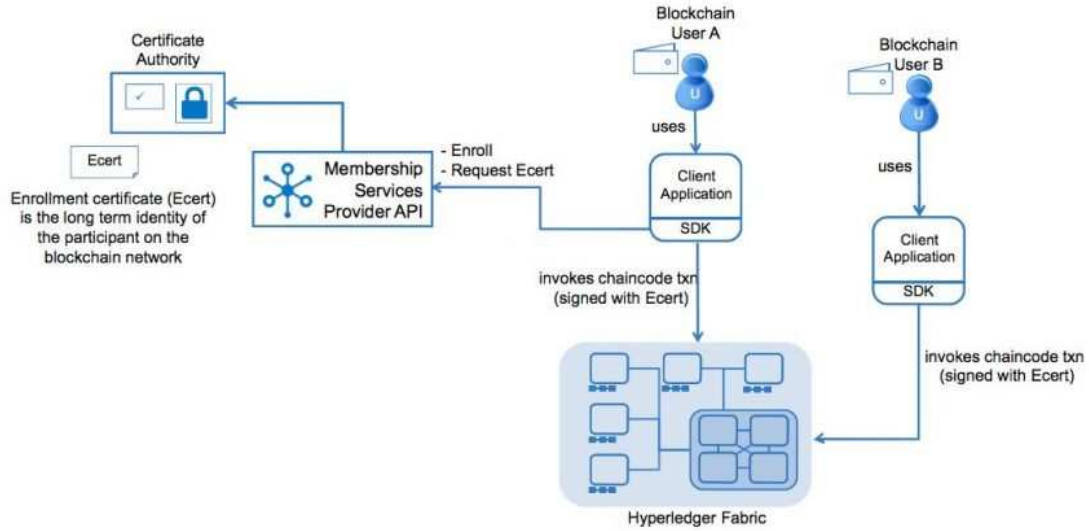
Ilustración 12. Ejemplo de tipos de roles por interesado



Fuente: Elaboración Propia

Se hace necesario un identificador de los entes que interactúan con la cadena de bloques asignado por una institución que otorgue membresía, debido a que existen solicitudes de acceso que deben ser manejadas por el paciente, el médico o el hospital llegando a la conclusión de la sección 4.1.4 donde se indica que debemos usar una Cadena de bloques de tipo Autorizada para conocer la identidad de todos los nodos [9]. Una solución es usar un Proveedor de servicios de membresía o MSP [10] que defina las reglas que rigen las identidades válidas para una organización tal como se muestra en la figura de abajo. La implementación predeterminada de un MSP utiliza certificados X.509 como identidades, adoptando un modelo jerárquico tradicional de Infraestructura de clave pública o PKI.

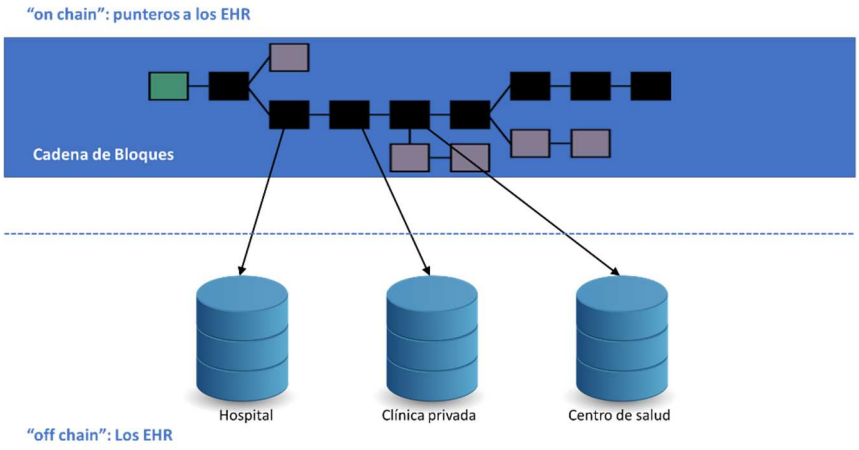
Ilustración 13. Hyperledger Fabric MSP



Fuente: [38]

Además, los tamaños de los registros clínicos pueden requerir grandes cantidades de almacenamiento, considerando que se deben replicar grandes cantidades de datos y existirán lugares remotos con limitación en el ancho de banda [39], lo cual nos lleva a un problema de escalabilidad [40]. En conclusión, se debe diseñar la cadena de bloques para que únicamente registre enlaces a la información de la base de datos que originó el registro, es decir un puntero o registro *on-chain* hacia el registro de los datos *off-chain* [24].

Ilustración 14. Escalabilidad de la cadena de bloques para soportar enormes cantidades de datos



Fuente: Elaboración propia

Otra consideración de diseño es la privacidad por lo cual toda comunicación entre los nodos debe ser cifrada para que los datos o referencias hacia los datos de los pacientes no vayan en texto claro, para Hyperledger Fabric se usa TLS [41] entre los *peers*.

5.3.3 Diseño final de la solución con Hyperledger

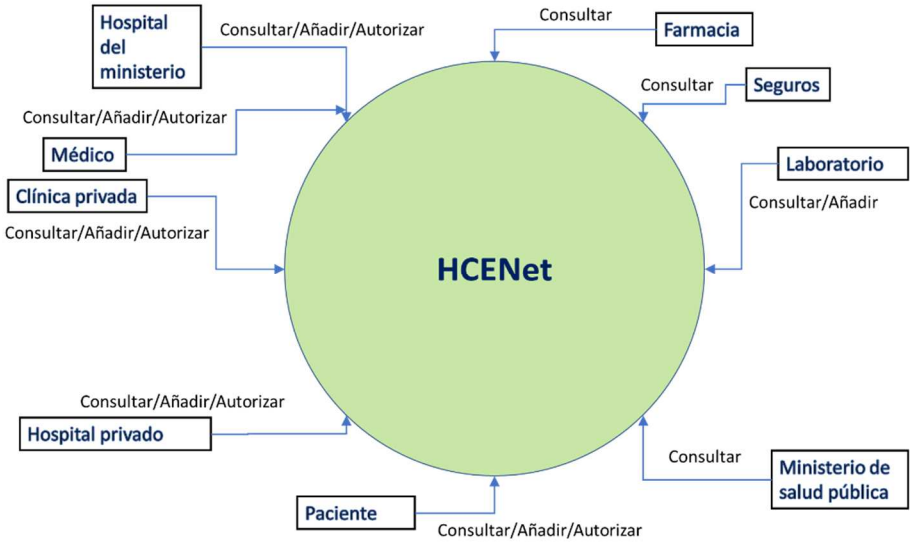
Hyperledger Fabric, también llamado 'Fabric', es un *framework* o marco de trabajo de código abierto para implementar *blockchains permissioned* o Cadena de bloques autorizadas. Digital Asset e IBM fueron las dos compañías que construyeron la versión inicial de *Fabric*. Usando este marco de trabajo se realizaron todos los diseños que se verán a continuación bajo la red de Historias Clínicas Electrónicas o HCENet:

Participantes

Los participantes son miembros de una red empresarial, pueden poseer activos y presentar transacciones. En la figura abajo se describe la red HCENet que permite a los participantes debidamente autorizados realizar algunas acciones descritas a continuación:

- Consultar. Permite a un participante consultar registros cargados sobre la red HCENet. La información consultada corresponderá al canal que pertenezca el *peer* y la entidad que ejecuta la transacción.
- Escribir. Permite a un participante añadir nuevos registros médicos sobre la red HCENet sobre un paciente en particular. La información registrada corresponderá al canal que pertenezca el *peer* y la entidad que ejecuta la transacción.
- Autorizar. Permite de forma automática autorizar a un participante para consultar registros médicos de un paciente.

Ilustración 14. Acciones que pueden realizar los participantes sobre la red HCENet



Fuente: Elaboración propia

Los tipos de participantes se modelan al igual que los activos, así que deben tener un identificador y pueden tener otras propiedades según sea necesario. Un participante puede tener una o más identidades. Así para nuestra solución definiremos los siguientes ejemplos:

Ilustración 15. Propiedades ejemplo de dos participantes de la red HCENet

Paciente	
pacienteID	String
dni	String
nombres	String
apellidos	String
fecha_nacimiento	Datetime
estado_civil	String
conyugueDNI	String
padreDNI	String
madreDNI	String
género	String

Médico	
médicoID	String
dni	String
nombres	String
apellidos	String
fecha nacimiento	Datetime
número de colegiado	String

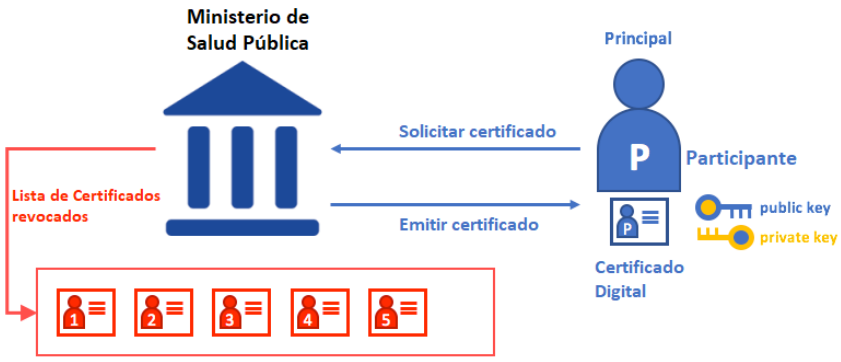
Fuente: Elaboración propia

Identidades

Las identidades se definirán para cada uno de los participantes de nuestra solución, esto es imprescindible porque determinan los permisos exactos sobre los recursos y el acceso a la HCE que los actores tienen en una red *blockchain*. Además, una identidad digital tiene algunos atributos adicionales que *Fabric* usa para determinar los permisos. A la unión de la

identidad y los atributos asociados se le conoce como *Principal*. Los *Principals* son como los identificadores de usuario o los identificadores de grupo, pero un poco más flexibles porque pueden incluir una amplia gama de propiedades de la identidad de un actor, como la organización, la unidad organizativa, el rol o incluso la identidad específica del actor. Las identidades serán emitidas por una autoridad certificadora (CA) personalizada para *Hyperledger* la cual es *Fabric-CA*. Tal como se muestra en la figura de abajo será manejado por la PKI interna de Hyperledger Fabric-CA, la cuál será administrada por el Ministerio de Salud Pública del Ecuador.

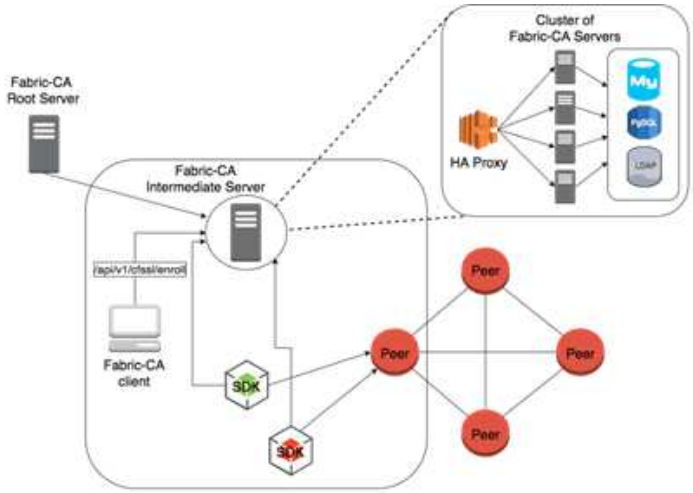
Ilustración 16. Fabric-CA para HCENet



Fuente: Elaboración propia

Todas las identidades serán manejadas por un clúster de servidores intermedios Fabric-CA creados por un servidor Fabric-CA *root* que de desconectará por mejor práctica de seguridad [42] de tal forma que si es afectado un servidor intermedio solo se revocará su certificado y se crearán nuevos servidores intermedios Fabric-CA tal como muestra la figura abajo.

Ilustración 17. Hyperledger Fabric-CA



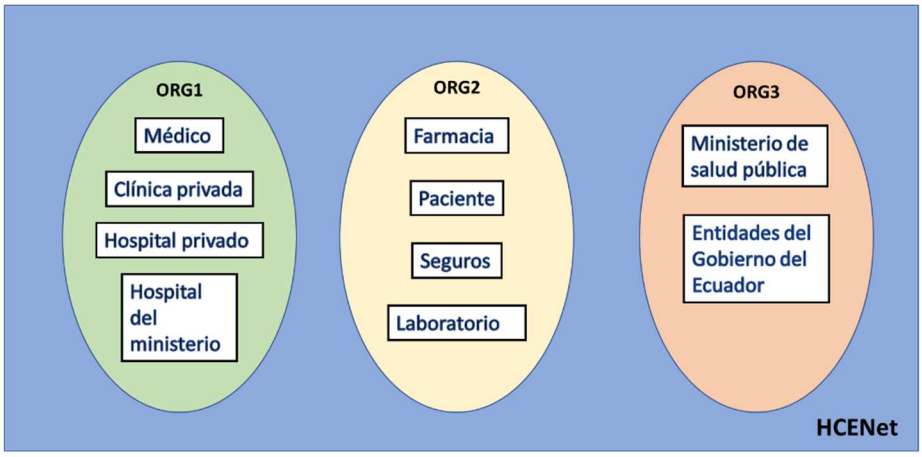
Fuente: [10]

Se deriva de la ilustración superior que la actividad de enrolamiento la debe realizar un participante. Para HCENet debe realizarla el administrador del Fabric-CA que es el Ministerio Público de Salud mediante un proceso automático.

Proveedor de servicios de membresía y Organizaciones pertenecientes a HCENet

Para la red HCENet existirá un MSP por cada organización bajo el control del Ministerio de Salud Pública. Bajo estas estructuras se crearán todas las identidades digitales usando las siguientes organizaciones tal como se muestra en la figura abajo:

Ilustración 18. Organizaciones creadas dentro del MSP1 de HCENet



Fuente: Elaboración propia.

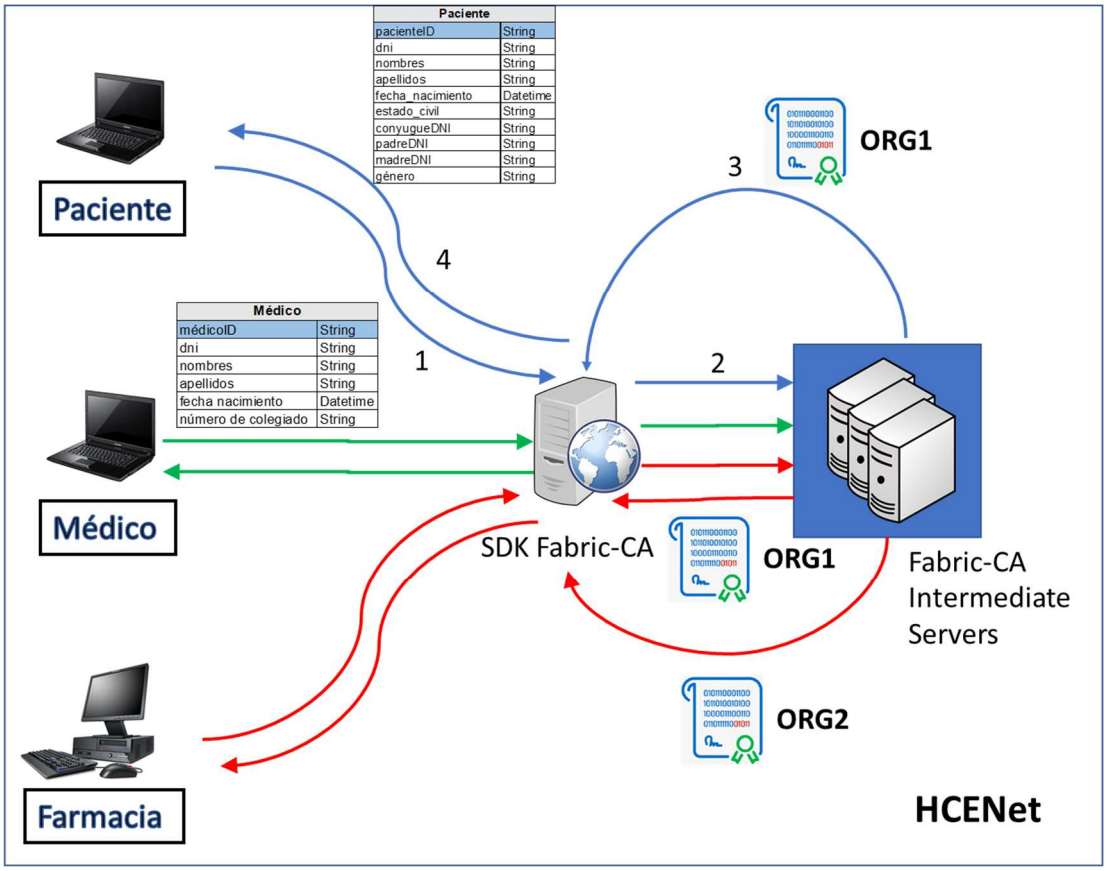
- Org1. Se usa para los participantes que tienen acceso a toda la HCE y pueden realizar todas las operaciones: consulta, escritura y autorización.
- Org2. Se usa para los participantes que tienen acceso a registros especiales como: diagnostico, prescripción de exámenes, prescripción de medicinas y costos asociados. En conclusión, solo pueden realizar operaciones de consultas de esos registros.
- Org3. Se usa para nodos especiales *orderer* o *commiters* que escriben los datos sobre los *ledgers*.

Enrolamiento de un participante en la red

El Ministerio de Salud Pública será el responsable de la administración y operación del *Fabric-CA*. Así mismo, administrará el enrolamiento o membresía emitiendo certificados para los nodos participantes en la cadena de bloques de Hyperledger y los Fabric Client. También generará las listas de control de acceso durante el establecimiento de los canales de acuerdo con los permisos o roles de usuarios. Se manejarán los tipos de accesos en los atributos de organización de los certificados. Para lo cual se deberá seguir los siguientes pasos como muestra la figura abajo:

- Paso 1. El participante accede al portal web del ministerio de salud e ingresa sus datos seleccionando uno de sus posibles roles: paciente, medico, farmacia, etc. El portal web validará la información ingresada y realizará su proceso de verificación
- Paso 2. Verificados todos los datos del participante usará el SDK del Fabric-CA para enrolar al usuario bajo el MSP correspondiente. Enviará la solicitud de enrolamiento contra un HA-Proxy que balanceará la carga contra los *Fabric-CA intermediate servers*.
- Paso 3. Los *Fabric-CA intermediate servers* emitirán un certificado digital correspondiente de acuerdo al perfil del participante, asignándole una organización apropiada Org1, Org2 u Org3.
- Paso 4. El portal web del ministerio de salud despachará las identidades digitales a los participantes.

Ilustración 15. Flujo de enrolamiento de un participante



Fuente: Elaboración propia.

Paso 5. Este paso consiste en registrar mediante un *chaincode* el ID del participante y su llave pública de tal forma que quedará un Ledger asociando el par (ID, llave pública) sobre un canal específico del cual hablaremos más adelante.

Todas las identidades tomarán su correspondiente organización y un tipo de rol dentro de cada MSP de acuerdo con la siguiente tabla:

Ilustración 16. Asignación de rol de la identidad dentro de la organización

MSP Role identity	
Tipo	ID
Miembro	0
Admin	1
Cliente	2
Peer	3

Fuente: Elaboración propia.

Donde 0 es un miembro por defecto del MSP, 1 es para administradores que tienen labores como administrar el canal y establecer políticas. El ID 2 es para aplicaciones o clientes creados que desean ejecutar transacciones. Por último, el ID 3 define el rol de peer que mantiene los *ledgers* y puede actuar como *endorser*, *orderer* o *commiter*.

Canales

Un canal sirve para que un subconjunto de miembros en la red realice transacciones, por lo que estos miembros conforman el conjunto de partes interesadas de las transacciones enviadas a este canal, y solo estos miembros pueden recibir los bloques que contienen las transacciones, que están completamente aislados de otras transacciones en otros canales. Un miembro que no está autorizado en un canal no puede unirse al canal y no puede realizar transacciones en ese canal. Para HCENet se definirán 3 canales para mantener la privacidad de los datos:

- Canal 1. Mantiene los punteros a las HCE y tiene las tablas de estado y el registro histórico de todos los registros médicos.
- Canal 2. Solo mantiene los punteros hacia los siguientes registros: Diagnósticos, prescripciones médicas y ordenes de exámenes. Así mismo contendrá las tablas de estado y el registro histórico de transacciones.
- Canal 3. Están los peers que pertenecen al *Order Service* u *orders peers*. Y existen *peers* adicionales que mantienen las parejas (ID, llave pública) de los registros de identidades.

Estructura final de HCENet

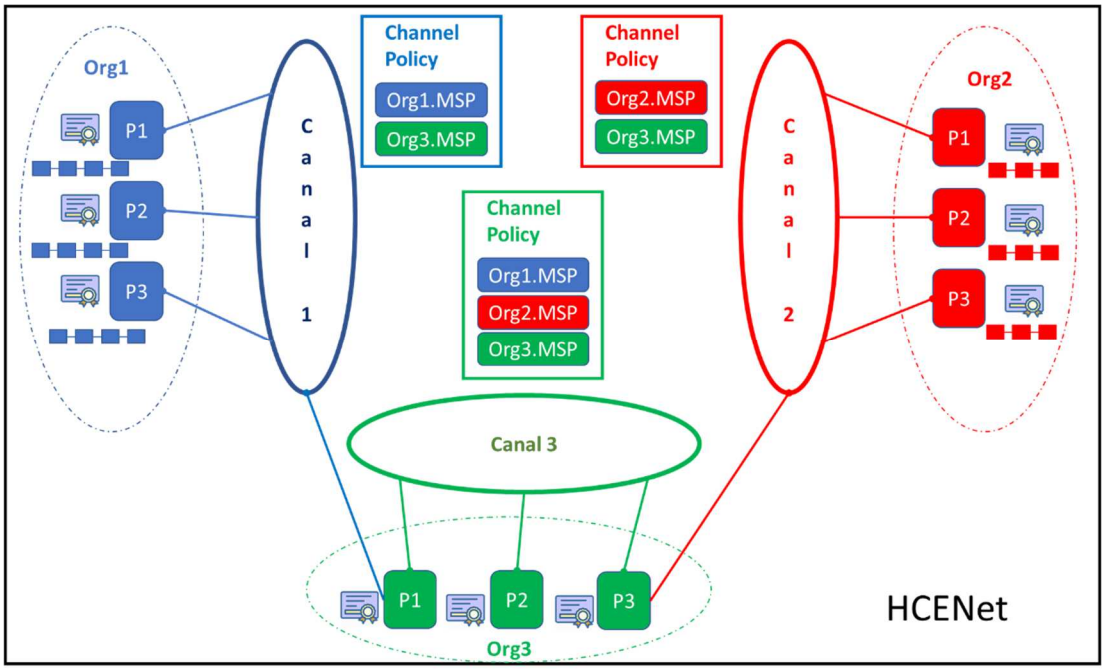
Con todas las definiciones de participantes, identidades, MSP/organizaciones y canales ya podemos definir la estructura final de la red de negocios HCENet que muestra en la siguiente figura:

- Cada Canal deberá tener sus propias aplicaciones desarrolladas bajo el SDK de Hyperledger Fabric.
- Cada Canal deberá configurarse con su propio con al menos 2 MSPs para poder validar las identidades de los nodos que no pertenecen al canal. Tenemos así:

- Canal 1 se compone de Org1.msp y Org3.msp, de tal forma que puede validar las identidades propias de su canal 1 más la identidad del peer *orderer* que reside en la Org3.
- Canal 2 se compone de Org2.msp y Org3.msp, de tal forma que puede validar las identidades propias de su canal 2 más la identidad del peer *orderer* que reside en la Org3.
- Canal 3 se compone de Org1.msp, Org2.msp y Org3.msp para poder validar las identidades de las 3 organizaciones, debido a que todos los nodos *orderer* residen en Org3.

- Cada peer tendrá su propio *Ledger* que consta de la tabla del estado actual y el registro histórico. Cuando el peer tenga más de un canal asociado tendrá más de un *Ledger*.

Ilustración 17. Estructura final de HCENet



Fuente: Elaboración propia.

Como se puede ver arriba en la figura y ya concluimos en las consideraciones de diseño los registros médicos deben estar fuera de la cadena de bloques para que sea una solución escalable. En la sección de *Chaincode* se establecerá como interactúa los registros de HCE *off-chain* contra los registros de la HCE *on-chain*.

Chaincodes

A continuación, analizaremos los chaincodes o contratos inteligentes que se deberán implementar en cada canal para poder realizar escrituras, consultas sobre la cadena de bloques especifica de cada canal.

Primero debemos entender el contexto en que habita la información, para lo cual daremos un ejemplo:

- Una persona ingresa por emergencia a un hospital público en Ecuador. Como primer paso se le toman los datos como el documento nacional de identificación. Los hospitales toman ese valor como clave y generan un numero de historia clínica de uso interno. En este punto se ejecutará un *chaincode* "buscar_participante" que mediante el ID del paciente o su DNI obtendrá el valor de su llave pública.
- Internamente le tomaran sus datos vitales y se creará un registro de datos vitales en los sistemas internos. Este primer registro se escribirá en la base de datos local interna del hospital. Como paso adicional se publicará un identificador de recursos uniforme o URI con el atributo de consulta configurado con el hash del URI, más el atributo de tipo de registro. Por último, un atributo de consulta adicional que será un contador. De tal forma que el atributo URI apuntará a la información interna de la base de datos.
- Para todas las demás interacciones como orden de exámenes, consulta, diagnóstico y prescripción de medicina se deberá guardar el registro en la base interna y generar el URI que contenga todos los campos citados antes.
- Un cliente con el SDK de *Hyperledger Fabric* escuchará cada evento en la base de datos del hospital y registrará en HCENet cada URI usando el chaincode "escribir_EHR". La URI se cifrará usando la llave privada del hospital y luego se cifrará nuevamente usando la llave pública del paciente.

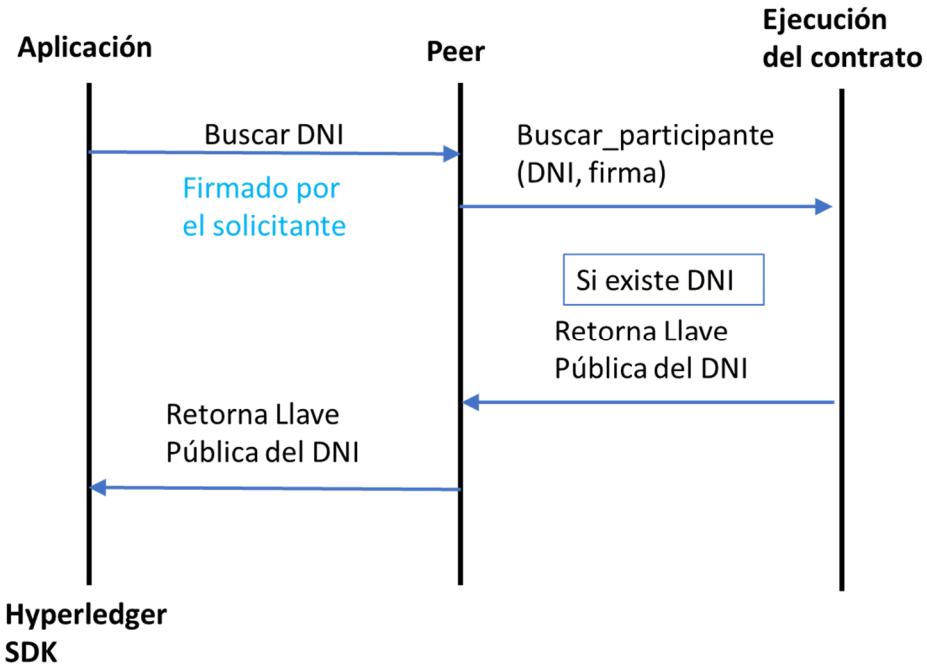
Con este ejemplo entendemos que la información real de toda una asistencia médica reside *off-chain* y sobre la solución de la cadena de

bloques *on-chain* solo residen punteros cifrados hacia el origen de datos.

Chaincode “Buscar_participante”. Este contrato se instala en todos los *peers* de los canales. Funciona tal como muestra la figura abajo:

- Usa como parámetros el DNI del participante buscado y la firma con su llave pública.
- El peer verifica la identidad del solicitante y compara contra los permisos del *chaincode* para revisar si tiene la autorización de ejecutar la búsqueda sobre el *Ledger*. Una vez verificado ejecuta el contrato sobre la cadena.
- El contrato retorna como resultado la llave pública del DNI buscado en caso de existir, caso contrario debe emitir un error de “usuario no encontrado”

Ilustración 18. *Chaincode* Buscar_participante



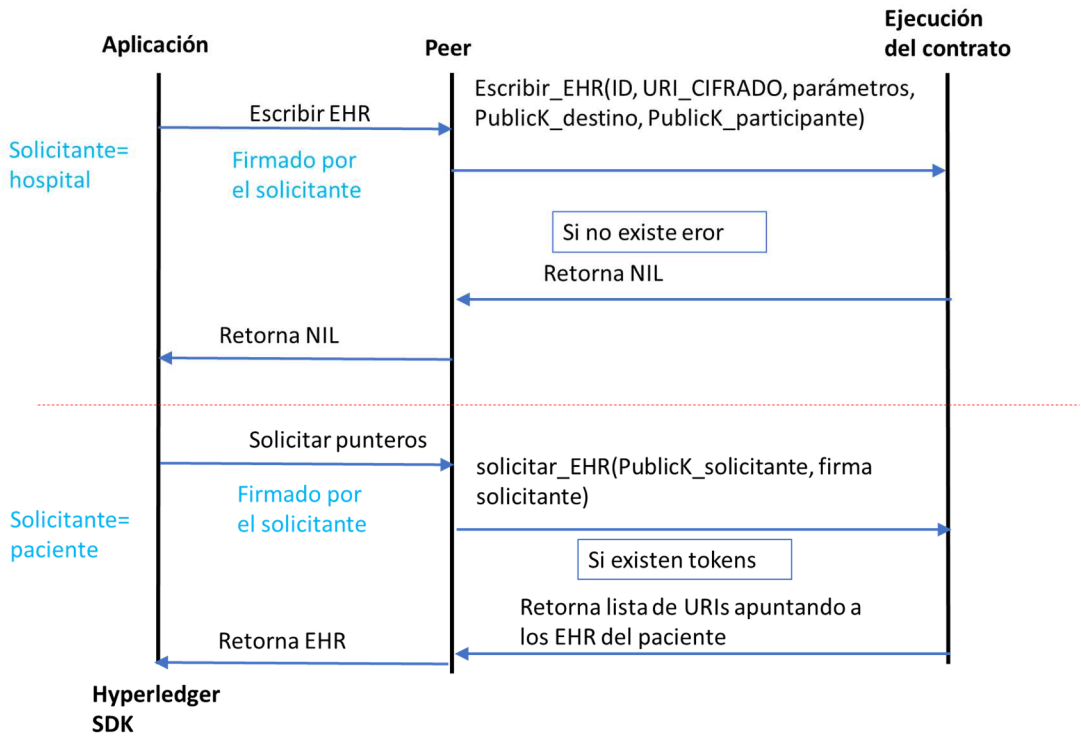
Fuente: Elaboración propia.

Chaincode “Escribir_EHR” y “Solicitar_EHR”. Este contrato se instala sobre los *peers* del canal 1 y permite escribir registros sobre el Ledger. Tal como se muestra en la figura de abajo:

- La operación comienza cuando un ente de salud ha realizado un registro en su sistema local y se dispara una inserción sobre HCENet, para lo cual forma un URI apuntando a los datos internos.
- La aplicación solicitará a un *peer* la ejecución del chaincode Escribir_EHR para lo cual la aplicación deberá enviar algunos parametros como:
    - URI cifrado = URI cifrado con la llave privada del emisor y el resultado se lo debe cifrar con la llave pública del paciente.
    - Hash del URI en texto claro.
    - Contador.
    - Llave pública del paciente o destino del URI.
    - Está implicito que se debe enviar la identidad digital del solicitante para que se autorice la ejecución del chaincode.
- Una vez ejecutado el chaincode el resultado será un “nil” que equivale a un nulo. Caso contrario retornará un error.

De está forma se poblará el ledger con los tokens asignados a una llave público de destino o del paciente en este caso.

Ilustración 19. Inserción y recuperación de punteros de EHR en HCENet



Fuente: Elaboración propia.

Para continuar tal como se muestra en la figura superior el paciente puede obtener en cualquier momento los URI de sus EHR. Usando el *chaincode* “Solicitar_EHR” para lo cual deberá adjuntar su llave pública para recuperar los registros cargados y obviamente su certificado digital para poder ejecutar el *chaincode*. En caso de tener tokens cargados la función retornará los valores: URI cifrado, Hash del URI y el contador.

Este mismo *chaincode* se lo puede extender para que el hospital comparta los registros de tipo: orden de laboratorio, prescripciones médicas, etc. hacia los destinos que son laboratorio y farmacia. Solo se debe tener en cuenta que no se usa DNI para la búsqueda de sus claves públicas. Inclusive el mismo chaincode sirve para compartir historias clínicas entre hospitales, médicos y demás entes de salud.

Conclusiones

Como contribución original de nuestro trabajo se puede acotar que el diseño HCENet cumple con HIPAA [36] y el Acuerdo Ministerial 9 del Ministerio de Salud Pública del Ecuador [14] para el manejo de históricas clínicas electrónica, ya que el uso de *blokchain* garantiza la firma digital no solo del profesional de salud sino de todos los actores que intervienen en su acceso para lectura o escritura. En cada uno de los principios que la ley señala de la siguiente manera:

- Integridad de la información. La integridad se mantiene bajo el funcionamiento del *Ledger* en su capa *blockchain con el respectivo hashing y encadenamiento hacia atrás*. Esto es una característica implícita de HCENet.
- Autenticidad. El uso de la firma electrónica bajo un esquema de autoridad certificadora del MSP garantiza la autenticidad de la información contenida en la cadena de bloques. Adicional, se recomienda el uso de una CA externa como la que provee el Banco Central del Ecuador [43].
- Confidencialidad. El diseño garantiza mediante las organizaciones, los canales y el *chaincode* que solo el personal

autorizado tendrá acceso a los punteros donde reside la información.

- Exactitud e Inteligibilidad. Estos puntos no están cubiertos por nuestro diseño debido a que sólo contiene los punteros hacia la información.
- Disponibilidad. El diseño propuesto provee disponibilidad debido a que los *ledgers* existen en todos los *peers* de la red, esto es una característica implícita de *blokchain*. Pero desde el punto de vista práctico puede fallar el acceso al origen de datos o la información en sí.
- Pertinencia. No está cubierta en nuestro diseño. La pertinencia es una característica que debe ser considerada en la toma de información médica por el profesional de salud.

Otra contribución de nuestro trabajo es la simplicidad del diseño que se reduce a pocos métodos que satisfacen todos los escenarios, se podría pensar que hace falta una función “QueryALL” o “Consulta_todo” para compartir los registros que un paciente recupero de un hospital. Pero en realidad la solución simple es que el paciente tenga todos los URI cargados en su aplicación móvil o *Wallet*. Así, para compartir su historia lo único que debería hacer es “Escribir_EHR” hacia la llave pública del destino, pero eso generaría duplicidad de registros lo cual crea un problema de escalabilidad del *Ledger*. Para estos casos la conclusión lógica es crear una nueva cadena en otro canal que solo sirva para compartir las URI entre entidades de salud.

En concordancia con lo antes expuesto nuestro diseño soluciona el control de accesos a la HCE con ciertas restricciones, pero se mantiene constante el peligro de la modificación de los datos en los orígenes que se encuentran bajo la administración de un ente de salud. Para fines teóricos a un médico el sistema le indicará que los EHR no tienen integridad o han sido modificados, pero para fines prácticos el paciente no será atendido con toda la información necesaria para un buen diagnóstico. Es decir, no soluciona uno de los puntos primordiales de la HCE que es poder evaluar al paciente con toda la información disponible y veraz.

Resultado del presente diseño también se derivan dos riesgos que describiremos a continuación:

- Luego de revisar internamente el funcionamiento de Hyperledger y como se adapta a la solución de HCE podemos concluir que es una solución con centralización en dos puntos claves: Autorización de usuarios para unirse a la red y el algoritmo de consenso que es centralizado desde el punto de vista que solo un grupo de nodos *orderer* están permitidos en indicar las transacciones que se deben asentar la cadena de bloques. Por consiguiente, volvemos al punto de centralización y confianza. Uno de los potenciales problemas de la centralización es que un ataque al servicio MSP podría crear un grupo de nodos *Orderer* para modificar las cadenas de bloques creadas sobre cada canal. Se pierde en cierta medida la garantía de integridad y confidencialidad de la información. Cabe destacar que el ataque de modificación solo afectará desde el ultimo bloque hacia adelante, lo escrito atrás ya se vuelve inmutable por el encadenamiento hacia atrás propio de la Cadena de bloques.
- Es muy importante notar que la solución funciona para administrar el acceso a la HCE de un paciente, pero se debe dar solución al problema de secuencia de los datos. El origen de los datos debe clasificar los registros de información e invocar un *chaincode* para añadirlos en el orden que se vayan dando, en caso de realizarlos en modo lote o *Batch* existirá la duda de cual registro se originó primero. En resumen, una colección de registros añadidos en desorden podría confundir o hacer que el tratante de salud realice un diagnostico errado sobre el paciente. También debemos analizar que nuestra solución HCENet no puede garantizar accesos granulares, es decir el acceso a registros específicos de información, ya que se almacena el puntero a todos los eventos generados por cada atención médica que podría contener muchos tipos de registros.

Como próximos trabajos se deben evaluar:

- Una técnica o proceso para migrar las HCE actuales que no estarían subidas a la red HCENet.
- Mejorar el proceso de enrolamiento para que se ejecute como una condición en la inscripción de un paciente recién nacido, de tal forma que obtenga su identidad digital desde el principio de su vida.
- Un método para clasificar la información en el origen *off-chain* para garantizar el acceso a la información específica requerida a través de los punteros *on-chain*.

Bibliografía

[1] Canadian Medical Protective Association , «Electronic Records Handbook,» 2014. [En línea]. Available: https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/handbooks/com_electronic_records_handbook-e.pdf. [Último acceso: 2018 12 11].

[2] Canadian Medical Protective Association, «Can border agents search your smartphone? Considerations for protecting patient information on mobile devices when crossing international borders,» enero 2019. [En línea]. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2019/can-border-agents-search-your-smartphone. [Último acceso: 1 febrero 2019].

[3] F. Casino, T. K. Dasaklis y C. Patsakis, «A systematic literature review of blockchain-based applications: Current status, classification and open issues,» *Telematics and Informatics,* vol. 36, nº 2019, pp. 55-81, Marzo 2019.

[4] J. Aguirre, «Cadena de bloques: potencial aplicación a historias clínicas electrónicas,» 2017. [En línea]. Available: http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-0976_AguirreRegatoJA. [Último acceso: 30 01 2019].

[5] Bitcoin, «Bitcoin,» Bitcoin, [En línea]. Available: https://bitcoin.org/es/descargar. [Último acceso: 27 04 2017].

[6] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher y F. Wang, «Secure and Trustable Electronic Medical Records Sharing using Blockchain,» de *AMIA Annual Symposium Proceedings*, 2016.

[7] V. Buterin, «Ethereum: The Ultimate Smart Contract and Decentralized Application Platform,» 2013. [En línea]. Available: http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html. [Último acceso: 14 febrero 2019].

[8] E. Androulaki, A. Barger , V. Bortnikov , C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou , M. Vukolić y J. Yellick, «HyperledgerFabric:ADistributedOperatingSystemfor PermissionedBlockchains,» de *EuroSysEuropean Conference on Computer Systems*, Porto, Portugal, 2018.

[9] C. Cachin, «Architecture of the Hyperledger Blockchain Fabric,» julio 2016. [En línea]. Available: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf. [Último acceso: 11 mayo 2019].

[10] Hyperledger 2019, «Hyperledger Fabric,» Hyperledger 2019, [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/identity/identity.html. [Último acceso: 14 Noviembre 2019].

[11] S. Maheshwari, «Aspectos básicos de blockchain: Hyperledger Fabric e Hyperledger Composer,» IBM, 14 Diciembre 2018. [En línea]. Available: https://www.ibm.com/developerworks/ssa/library/cl-blockchain-hyperledger-fabric-hyperledger-composer-compared/index.html. [Último acceso: 25 Febrero 2019].

[12] Republica del Ecuador, «CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008,» 20 10 2008. [En línea]. Available: http://www.inocar.mil.ec/web/images/lotaip/2015/literal_a/base_legal/A._Constitucion_republica_ecuador_2008constitucion.pdf. [Último acceso: 28 01 2019].

[13] Asamblea Nacional de la República de Ecuador, «Ley Orgánica de Salud,» 23 10 2018. [En línea]. Available: https://www.asambleanacional.gob.ec/es/system/files/ley_organica_reformatoria_a_la_ley_organica_de_salud_ley_67_para_incluir_el_tratamiento_de_las_enfermedades_raras_o_huerfanas.pdf. [Último acceso: 26 02 2019].

[14] Ministerio de Salud Pública del Ecuador, «REGLAMENTO PARA EL MANEJO DE LA HISTORIA CLINICA ELECTRONICA,» 22 03 2017. [En línea]. Available: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/registro-oficial/item/9000-registro-oficial-no-968.html. [Último acceso: 2019 02 20].

[15] Asamblea Nacional de la Republica del Ecuador, «Proyecto de Ley Orgánica de la Protección de los Derechos de la Intimidad y Privacidad sobre los Datos Personales,» 12 07 2016. [En línea]. Available: https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/250%20protec-intimidad-grivadeneira-12-07-2016/PP-protec-intimidad-grivadeneira-12-07-2016.pdf. [Último acceso: 19 01 2019].

[16] Department of Health and Human Services, United States of America, «HITECH,» 18 02 2009. [En línea]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html. [Último acceso: 30 01 2019].

[17] El Parlamento Europeo y el Consejo de la Unión Europea, «REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO,» 27 04 2016. [En línea]. Available: https://www.boe.es/doue/2016/119/L00001-00088.pdf. [Último acceso: 03 02 2019].

[18] G. Zyskind, O. Nathan y A. Pentland, «Decentralizing Privacy: Using Blockchain to Protect,» de *2015 IEEE CS Security and Privacy Workshops*, Washington D.C., 2015.

[19] A. Ekblaw, A. Azaria, J. Halamka y A. Lippman, «A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data,» MIT Media Lab, Massachusetts, 2016.

[20] Office of the National Coordinator , «Blockchain Challenge,» Innovation Center, 7 julio 2016. [En línea]. Available: http://www.cccinnovationcenter.com/challenges/block-chain-challenge/. [Último acceso: 23 septiembre 2017].

[21] Office of the National Coordinator for Health IT, «Shared Nationwide Interoperability Roadmap,» 2015. [En línea]. Available: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. [Último acceso: 23 septiembre 2017].

[22] Q. Xia, E. Boateng, K. Omono , J. Gao, X. Du y M. Guizani, «MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,» *IEEE,* vol. 5, pp. 14757 - 14767, 2017.

[23] A. Roehrs, C. A. Costa y R. da Rosa Righi, «OmniPHR: A distributed architecture model to integrate personal health records,» *Journal of Biomedical Informatics,* vol. 71, pp. 70-81, 2017.

[24] P. Zhang, J. White, D. C. Schmidt, G. Lenz y S. T. Rosenbloom, «FHIRChain: Applying Blockchain to Securely and Scalably Share,» *Computational and Structural Biotechnology Journal,* vol. 16, nº 2018, pp. 267-278, 2018.

[25] R. Hales Hylock y X. Zeng, «A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study,» *J Med Internet Res,* vol. 21, nº 8, 2019.

[26] J. Heinrich , C. Fitte y F. Teuteberg, «Towards a Stakeholder-Oriented Blockchain-Based Architecturefor Electronic Health Records: Design Science Research Study,» *JOURNAL OF MEDICAL INTERNET RESEARCH,* vol. 21, nº 10, 2019.

[27] K. Wüst y A. Gervais, «Do you need a Blockchain,» de *2018 Crypto Valley Conference on Blockchain Technology*, 2018.

[28] D. Birch , R. G. Brown y S. Parulava, «Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis,» *Journal of Payments Strategy & Systems,* vol. 10, nº 2, pp. 118-131 (14), 2016.

[29] CompTIA’s Blockchain Advisory Council , «CompTIA Blockchain Decision Tree,» 1 Noviembre 2019. [En línea]. Available: https://www.comptia.org/content/infographic/blockchain-decision-tree. [Último acceso: 3 Enero 2020].

[30] J. Pearson, «Millions of Dollars In Ethereum Are Vulnerable to Hackers Right Now,» 22 febrero 2018. [En línea]. Available: https://motherboard.vice.com/en_us/article/8xddka/millions-of-dollars-in-ethereum-are-vulnerable-to-hackers-right-now-smart-contract-bugs. [Último acceso: 15 febrero 2019].

[31] A. J. Menezes, P. C. Van Oorschot y S. A. Vanstonne, Handbook of Applied Cryptography, CRC Press, 1996.

[32] A. Hevner, «A Three Cycle View of Design Science Research,» *Scandinavian Journal of Information Systems,* vol. 19, nº 2, pp. 87-92, 2007.

[33] A. Hevner, S. March, J. Park y S. Ram, «Design science in information systems research,» *MIS Quarterly,* vol. 28, nº 1, pp. 75-104, 2004.

[34] A. Saquero, I. De la Torre y A. Durango, «Análisis de Aspectos de Interés sobre Privacidad y Seguridad en la Historia Clínica Electrónica,» *RevistaeSalud.com,* vol. 7, nº 27, 2011.

[35] J. Rodrigues, I. De la Torre y G. Fernandez, «Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems,» *Journal of Medical Internet Research,* vol. 15, nº 8, 2013.

[36] U.S. Department of Health and Human Services, «Health Insurance Portability and Accountability Act of 1996 Security Rule,» 2003. [En línea]. Available: https://www.hhs.gov/hipaa/for-professionals/security/index.html. [Último acceso: 30 Octubre 2019].

[37] D. Ferraiolo, j. Cugini y R. Kuhn, «Role-based access control (RBAC): Features and motivations,» de *Proceedings of the 11th Annual Computer Security Applications Conference*, New Orleans, Louisiana, United States, 1995.

[38] A. Davies, «Pros and Cons of Hyperledger Fabric for Blockchain Networks,» DevTeam.Space, Agosto 2018. [En línea]. Available: https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-blockchain-networks/. [Último acceso: Octubre 2019].

[39] R. LaRose, S. Strover, J. Gregg y J. Straughbaar, «The impact of rural broadband development: Lessons from a natural field experiment,» *Government Information Quarterly,* vol. 28, nº 1, pp. 91-100, 2011.

[40] P. Zhang, J. White, D. Schmidt, G. Lenz y T. Rosenbloom, «FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,» *Computational and Structural Biotechnology Journal,* vol. 16, pp. 267-278, 2018.

[41] Internet Engineering Task Force (IETF) , «The Transport Layer Security (TLS) Protocol Version 1.3,» Agosto 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8446. [Último acceso: 22 Octubre 2019].

[42] I. Jeun, J. Park, T. Choi, S. Park, B. Park, B. Lee y Y. Shin, «A Best Practice for Root CA Key Update in PKI,» de *International Conference on Applied Cryptography and Network Security*, Berlin, 2004.

[43] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [En línea]. Available: www.bitcoin.org. [Último acceso: 12 Octubre 2016].

[44] D. Fernández, «Características criptográficas y potenciales debilidades de la criptodivisa Bitcoin,» Universidad de Buenos Aires, Buenos Aires, 2015.

[45] X. Liang, J. Zhao, S. Shetty, J. Liu y D. Li, «Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications,» de *The 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC 2017)*, Quebec, 2017.

Tabla de Figuras

Índice de Tablas