Patientory: Una red punto a punto para el cuidado de la salud por medio del almacenamiento de Registros Médicos Electrónicos v.1.1

Abstract

Un intercambio de información de salud (Health Information Exchange, HIE) basado en una blockchain puede demostrar un verdadero valor en la interoperabilidad y ciberseguridad. Este sistema tiene el potencial de eliminar la fricción y los costos de los intermediarios, cuando se considera la gestión de la salud de la población. Existen promesas de mejora de integración de los datos, reducción de costos por transacción, descentralización y desintermediación de confianza. Ser capaz de coordinar el cuidado de un paciente por medio de una HIE con blockchain esencialmente disminuye la necesidad de algunos servicios innecesarios y pruebas duplicadas, con reducción de costos y mejoras en las ineficiencias del ciclo de cuidado continuo del paciente, mientras se adhiere a todas las reglas y los estándares HIPAA. Patientory es un protocolo centrado en el paciente y soportado en tecnología blockchain. Está cambiando la forma en la que los participantes del sistema de salud gestionan datos médicos electrónicos e interactúan con los equipos de cuidado clínico.

Introducción

¿Qué es Blockchain?

Es la tecnología detrás de la moneda digital bitcoin. El nacimiento de blockchain se remonta a una persona (o grupo) sin identificar, con seudónimo conocido como Satoshi Nakamoto. Desde 2009 blockchain ha ganado un uso más generalizado en la industria financiera, con una variedad de negocios y servicios soportados en blockchain que están entrando al mercado. La tecnología blockchain se usa para compartir un libro de transacciones a través de una red de negocios sin el control por parte de una única entidad. El libro distribuido facilita la creación de relaciones comerciales de costos eficientes donde virtualmente cualquier cosa de valor puede ser seguido y negociado sin requerir un punto central de control. La tecnología pone la privacidad y el control de los datos en las manos del individuo. La confianza e integridad es establecida sin apoyarse en intermediarios.

Infraestructura de Salud actual

Alinear el enfoque basado en "procedimientos" hacia un "tratamiento holístico del individuo" requiere que los Proveedores de Salud formen "redes" que trabajan juntas hacia el objetivo en común de mejorar el resultado de los tratamientos de los pacientes actualmente bajo su cuidado, pacientes en cuidados post-tratamiento o pacientes que estén entre tratamientos. La necesidad de cooperación entre proveedores de salud, pasando por especialistas, médicos de tratamiento primario, cuidadores y proveedores de bienestar (como nutricionistas y enfermeros de rehabilitación) resulta en un incremento del uso de tecnologías digitales. Aunque estas soluciones han mejorado significativamente el seguimiento y la eficiencia en la entrega de los cuidados de salud, también han resultado en crear almacenes de información separados, principalmente al hablar de los sistemas de registros médicos electrónicos (EMR).

Las organizaciones gubernamentales y de salud gastan mucho tiempo y dinero en la construcción y gestión de sistemas de información tradicionales, así como en sistemas de

intercambio de datos. Estas entidades requieren recursos para solucionar constantemente problemas, actualizar información, ejecutar medidas de respaldo y recuperación de información, así como extraer información para reportes. Las leyes federales y programas de incentivos han hecho que los datos de salud sean más accesibles, en parte por las dificultades de los hospitales al momento de realizar implementaciones EMR. Sin embargo, la gran mayoría de sistemas hospitalarios no pueden aún compartir su información en forma fácil ni segura. Como resultado de esto, los doctores pasan más tiempo escribiendo que hablando con sus pacientes. El agotamiento de los médicos pasó de un 45% a un 54% entre 2011 y 2014[1]1

Aunque existe la noción de información de salud individualizada tanto en el aspecto clínico como de bienestar, esta no ha sido bien llevada hacia planes de cuidado "personalizados". Más aún, aunque hay una gran cantidad de datos, el ecosistema de salud en general es incapaz de crear adecuadamente un valor o arriesgarse a trabajar con Big Data para ayudar a predecir mejor futuros episodios de un paciente.

Por tanto, para elegir entre las soluciones actuales creadas por la industria de tecnologías en salud, hay que decidirse entre cuidado, privacidad o fraude económico para los pacientes. Vemos este problema en expansión a medida que los datos creados por la industria crece. La tecnología segura de blockchain, sus propiedades y su naturaleza distribuida pueden ayudar a reducir el costo y aumentar la eficiencia de estas operaciones así como proveer una infraestructura segura viable

Relación Paciente - Proveedor

El nuevo paradigma de salud demanda la necesidad de un cuidado efectivo y óptimo de los pacientes para obtener mejores resultados de los tratamientos. Esto requiere que los principales proveedores de salud puedan coordinar activamente y colaborar con otros proveedores relacionados, así como organizaciones conexas, laboratorios y farmacias. En

últimas, para que esto funcione, los registros de los pacientes necesitan ser actualizados y modificados en una forma ágil.

El software de EMR actualmente prohíbe una efectiva relación paciente-proveedor. Los portales para pacientes ofrecen una interacción mínima entre ellos, como resultado de mantener su información separada. Más aún, este software sólo provee una capacidad limitada de intercambio de información de un sistema a otro y usualmente requiere un individuo designado que sea capaz de realizar esta transferencia de información. Esto ha llevado a un aumento en la cantidad de retrasos entre organizaciones durante la entrega de los cuidados para el paciente y ha resultado también en la reducción en general de la calidad de la entrega de los servicios. Igualmente, a medida que los proveedores gastan más de su tiempo envueltos en coordinación, su efectividad en el tratamiento de los pacientes ha disminuido y su carga laboral se ha incrementado significativamente, resultando en un impacto negativo en los resultados entregados a sus pacientes.

En adición, dado que muchos doctores no quieren que sus pacientes accedan a sus registros electrónicos (EHR), los pacientes toman una actitud pasiva en el seguimiento de su salud. Esto en últimas los hace sentir sin control y sin sentido de pertenencia sobre su información, llevando al paciente a sentirse frustrado y desconectarse de su cuidado. Aunque hay un reciente incremento en las

aplicaciones móviles de salud, que ayudan a los individuos a hacer un seguimiento de sus signos vitales y parámetros de bienestar, la novedad no se ha aprovechado para mejorar los cuidados del paciente, su adherencia al tratamiento o almacenamiento de los resultados obtenidos, ya que también se enfrentan a los retos de no estar integrados a los EHR.

Visión general del sistema

http://imgur.com/TdK2JRa

Estructura de Patientory

Los problemas actuales se resuelven usando la Red Blockchain Patientory. Los sistemas EMR tradicionales son estructuras centralizadas, vulnerables a violaciones de seguridad, sujetas a regulaciones estrictas y costos extra muy elevados. Implementando la infraestructura Blockchain de Patientory, los proveedores verán una eliminación de las brechas de seguridad y un canal para facilitar la coordinación con resultados visibles en la mejora general de la salud de los pacientes. En la figura se muestra un esquema que describe la infraestructura blockchain de Patientory y su interoperatividad entre pacientes y proveedores.

Implementación del sistema

Regulaciones HIPAA y guías de cumplimiento

Antes de cualquier discusión importante sobre implementaciones, deben cumplirse las restricciones de ley dadas por los mandatos del Acto de Responsabilidades y Portabilidad de Seguros de Salud de 1996 (Health Insurance Portability and Accountability Act, HIPAA). Las reglas de principal cumplimiento son: la Regla de Privacidad, la Regla de Seguridad y las Guías de Computación en la Nube. El propósito de este documento no es el de realizar una investigación completa de la ley HIPAA. Los elementos que son pertinentes a la implementación

y su discusión serán definidos y discutidos en más detalles en el momento que su aplicación sea relevante.

Regla de Privacidad

El modelo de negocio de Patientory requiere que los requerimiento de la Regla de Privacidad sean aplicados dado que es necesario el almacenamiento electrónico y la transmisión de información de salud privada. La aplicabilidad de la Regla de Privacidad se resume como: "La Regla de Privacidad: (aplica) a planes de salud, cámaras de compensación y para cualquier proveedor que transmita información en forma electrónica" [2]2. En adición a dichos participantes, aquellas partes que actúen en su nombre, como proveedores de servicios también son responsables por el cumplimiento HIPAA. Estos agentes se denominan Socios de Negocio (Business Associates, BA) y el documento legal que define las reglas y regulaciones que el BA debe cumplir es el Contrato de Socio de Negocios (Business Associate Contract). HIPAA ejerce requerimientos estrictos en la naturaleza de estos acuerdos.

Los puntos a resaltar, dada la investigación inicial, son aquellos requerimientos que especifican la autorización de uso, el uso de información des-identificada y la definición de información privada. La Información Privada de Salud (Private Health Information, PHI o ePHI para datos electrónicos) es definida como "toda la información identificable individualmente, contenida o transmitida por una entidad cubierta o su socio de negocios, en cualquier forma o medio, sea electrónico, papel u oral"[2]2. La información de salud des-identificada es definida de la siguiente manera: "Información de Salud que no identifica a un individuo y con respecto a la cual no existe una base razonable para creer que la información puede usarse para identificar un individuo, no es información de salud identificable a un individuo"[2]2. Datos des-identificados usan restricciones que son resumidas por lo siguiente: "No hay

restricciones en el uso o publicación de información de salud des-identificada. La información de salud des-identificada no identifica ni provee una base razonable para identificar un individuo"[3]3. El límite de información identificada a des-identificada está definido como cualquier información que pueda restringir el posible número de individuos, al que una recolección de datos está asociada, con no menos del 0.04% del total de la población de EEUU.

Regla de Seguridad y Guías de Computación en la Nube

Dada la longitud del contenido asociado a este tema, solo aquellos elementos de aplicabilidad principal son nombrados para su referencia. Estos elementos de aplicabilidad primaria son los siguientes: "Cuando una entidad cubierta utiliza los servicios de un CSP para crear, recibir, mantener o transmitir ePHI (como en el caso de procesar o almacenar ePHI), en su nombre, el CSP es un socio de negocios bajo la HIPAA. Más aún, cuando un socio de negocios contrata un CSP para crear, recibir, mantener o transmitir ePHI en su nombre, el CSP subcontratado es un socio de negocios en sí mismo. Esto es cierto aún si el CSP procesa o almacena solamente ePHI encriptado y no tiene una llave de encripción para los datos. La falta de una llave de encripción no exime al CSP del estado de Socio de Negocios y sus obligaciones bajo las reglas HIPAA"[3]3.

Las entidades cubiertas a menudo usan Proveedores de Almacenamiento en la Nube (Cloud Storage Providers, CSP) para almacenar información de salud, a menudo citando que es más efectivo y reduciendo costos administrativos de infraestructura tecnológica. Sin embargo, a medida que los consumidores se apoyan en proveedores en la nube para almacenar sus datos personales, entregan el control directo sobre esos datos y, como resultado, no conocen quién tiene acceso y dónde está la información ubicada geográficamente. Aún si se desarrolla un acuerdo explícito entre el socio de negocios y el proveedor de almacenamiento en la nube, sólamente proveería los términos de quién toma la responsabilidad de la privacidad y la seguridad de los datos en el evento que ocurriera una brecha. El consumidor podría

potencialmente tener control sobre el acceso a estos flujos de datos, pero tendría que apoyarse en el proveedor de almacenamiento en la nube para hacer cumplir esos privilegios.

Aunque el uso de almacenamiento en la nube es popular, aún hay una cantidad de riesgos que el consumidor asume cuando se usa este mecanismo para su información personal. En una arquitectura basada en la nube, los datos son replicados y movidos constantemente, así que el riesgo de usos no autorizados de los datos se incrementa. Adicionalmente, varios individuos se les proporciona acceso potencial a los datos, como administradores, ingenieros de redes y expertos técnicos que ejecutan esos servicios en los servidores que almacenan estos datos. Esto incrementa el riesgo de acceso y uso no autorizado.

Sin embargo, aún si los datos se encuentran seguros por medio de controles de acceso restringidos y encriptación, en su punto de origen y mientras se encuentra en tránsito, aún se enfrentan a un problema para el desarrollo de Mediciones de Resultados Reportados por el Paciente (Patient-Reported Outcomes Measures, PROMs). El concepto de PROM es desarrollar una medición enfocada en el paciente que se relaciona con un área o enfoque que es de importancia para el paciente, y uno en el que su vinculación y retroalimentación es esencial para su implementación exitosa. Acceder a grandes flujos de datos de una variedad de dispositivos que son parte de las redes IoT, como se usan ahora, en unión con servicios basados en la nube pueden proveer una base sobre la cual constituir una PROM, pero es difícil saber si datos almacenados independientemente en la nube producirán una medida que tenga el significado esperado y relevancia para el paciente.

Implementar una tecnología blockchain para asegurar y mejorar la seguridad de los registros médicos asociados con el sistema, puede minimizar brechas de seguridad y la descentralización

final de la propiedad de los datos. El proceso de cifrado de datos se realiza al momento que llegan a la base de datos, mientras que el descifrado cuando van a ser utilizados. Los datos serán encriptados usando algoritmos que cumplen estándares NIST durante la transmisión y recepción como lo indica la ley. Por tanto, el intercambio de información cumplirá con las mejores prácticas delineadas por las especificaciones NIST.

En relación al rápido aumento de brechas de información que se enfrenta la industria de la salud, la tecnología blockchain permite el cumplimiento de HIPAA tanto para pacientes como proveedores

Análisis de limitaciones del sistema Blockchain debidas a las restricciones de HIPAA

La red Blockchain de Ethereum facilita un subconjunto diverso de implementaciones de sistemas debido a la aplicación de un lenguaje de programación Turing-completo que se ejecuta en la Máquina Virtual de Ethereum. Estos sistemas tienen limitaciones en el sentido que la máquina virtual no tiene una inspección directa desde el exterior, excepto por medio de Servicios Oráculo. Adicionalmente, las limitaciones de almacenamiento de la blockchain son aplicadas por el costo del almacenamiento y el costo del acceso a estos datos. En el momento de escribir este documento, el tiempo de bloque de la cadena establece un límite mínimo para solicitudes de cambio en el estado de al menos quince segundos.

La limitación de blockchain para almacenar información privada puede superarse por medio de ofuscación de los datos, como cifrado, pero en el evento que la llave para descifrar sea revelada, no hay forma de remover los datos sensibles de la blockchain. Para el propósito de llevar datos que cumplan con HIPAA, esto puede resultar potencialmente en una fuga de información constante e imposible de corregir dada la inmutabilidad de la blockchain misma. Aunque los datos des-identificados pueden, en teoría, ser guardados en la Blockchain Pública

de Ethereum, sería desastroso asumir que el mecanismo de des-identificación nunca fallará, o que la información asociada con interacciones en la blockchain no puedan, sin querer, revelar identidad. Esta conclusión es la misma a la que llegó el MIT Media Lab durante la formación de los Protocolos MedRec y se resume en el whitepaper MedRec[3]3. Minar esta información paralela puede ser tan simple como observar los tiempos e interacciones con contratos de almacenamiento conocidos.

Por medio de este análisis, puede ser posible asociar un individuo con una institución, y más importante, el tiempo durante el cual estuvo presente en las instalaciones. Dada la naturaleza especializada de algunas instalaciones, esta es información suficiente para constituir una violación de HIPAA dada la habilidad de un observador pasivo para inferir tanto identidad, ubicación, tiempo de interacción y, posiblemente, clase de diagnóstico.

Si se asume que esta ubicación está localizada en un punto remoto en la naturaleza, la reducción a menos de un 0.04% de la población de EEUU se convierte en un problema trivial. Estos hechos constituyen un punto único de falla que debe ser reconocido. Más aún, el almacenamiento directo de información, así sea cifrada, en una blockchain crea una responsabilidad de los administradores de base de datos para entrar en contratos BAC dadas sus acciones como una ubicación de almacenamiento de datos HIPAA (ver sección titulada &quo t;Regla de Seguridad y Guías de Computación en la Nube). Esta

es una expectativa irracional dado que cada minero e incluso los individuos con nodos pasivos necesitarían todos cumplir con la normativa HIPAA. Dados estos inconvenientes, nosotros implementamos un mecanismo de almacenamiento persistente de información sensitiva por medio de una implementación privada de una blockchain basada en Ethereum.

Objetivos de la implementación para Facilidad de uso y Seguridad

Los objetivos principales de cualquier sistema seguro pueden resumirse como los objetivos de confidencialidad, integridad, disponibilidad, responsabilidad y aseguramiento de la información e identidad. Para lograr estos objetivos un atacante y un usuario deben ser definidos. Cada uno de estos roles demanda cierto reconocimiento de habilidad. Desde la perspectiva del usuario, el sistema necesita ser suficientemente transparente de forma que no sea requerido un conocimiento avanzado. Igualmente, dada la inhabilidad de un usuario normal para comprender las complejas consideraciones de seguridad cibernética, el proceso necesita ser resistente a las acciones del usuario.

En el evento que un ataque ocurra, el sistema está creado de forma que la cantidad de trabajo que debe ser invertido para comprometer un recurso es más valioso que el valor del recurso mismo. Esto es, si se entiende que un participante avanzado con los recursos apropiados siempre será capaz de violar el sistema, dado suficiente tiempo y esfuerzo. Más resumidamente no hay defensa perfecta. Con estas restricciones, la implementación en sí misma puede ser ahora discutida de tal forma que logremos alcanzar los objetivos antes mencionados.

Definición de implementación de hardware y red

Para lograr los objetivos mencionados anteriormente, la implementación del sistema seleccionada requiere varios sistemas independientes. Cada sistema subdivide autoridad, se asegura que únicamente las entidades autorizadas puedan interactuar en una forma aprobada,

y provee un mecanismo para incrementar la seguridad mientras mantiene la disponibilidad. Este sistema también ha sido diseñado de forma tal que se pueda escalar desde el inicio, por medio de la adición de esquemas de llamados jerárquicos. Estos sistemas están descritos completamente y en detalle en las siguientes secciones.

La entidad con cara al público es una servidor para llamadas remotas (Remote Procedure Call, RPC) que actúa como una interfaz a una implementación privada de blockchain Ethereum (blockchain con permisos). Esta red de nodos blockchain únicamente está autorizada a interactuar con otros nodos blockchain, con un generador de llaves, con el sistema de almacenamiento HIPAA y el servidor RPC. La entidad generadora de llaves es el recurso que genera pares de llaves privadas / públicas para usar en la blockchain. El sistema de almacenamiento HIPAA guarda los datos que constituyen la información privada de salud ePHI.

Cuando una solicitud de datos ocurre, el sistema HIPAA puede obtener una autorización para comunicarse con el agente redireccionador, quien envía los datos hacia el servidor RPC. Alternativamente, puede estar estructurado de forma tal que el almacenamiento HIPAA se conecte directamente con el servidor RPC. Cada implementación tiene beneficios que deben ser considerados previamente a la selección final. En cualquier evento, el almacenamiento HIPAA descifra partes de la información relevantes al manejo de la solicitud. Esta información descifrada es luego cifrada nuevamente usando la llave pública del solicitante para su transmisión. Esta llave pública es también la llave pública del contrato que actúa como interfaz de control desde la blockchain hacia el almacenamiento HIPAA.

El diagrama de la topología de red especificada puede ser visto en la figura.
http://imgur.com/55iyWTu

Topografía de red Blockchain de Patientory

Definición de Implementación de Software

En adición a la separación física de los sistemas en la implementación de hardware y redes, el software de control de acceso facilita la integridad de los datos y las verificaciones de autorización de entidades solicitantes. El sistema de software, desde una perspectiva de control de acceso y cifrado de datos se describe abajo.

La base de datos HIPAA solo aceptará conexiones entrantes del redireccionador HIPAA. Esto asegura que el flujo de tráfico se separe únicamente por vías conocidas. El redireccionador HIPAA solo actuará para redireccionar una solicitud al almacenamiento HIPAA únicamente si ha ocurrido una transacción válida en la blockchain, y esta transacción resulta en la emisión de un evento de solicitud. Este evento debe contener la llave pública del solicitante, así como los campos solicitados. Finalmente, el servidor RPC usa una interfaz de aplicación (API) controlada de tal forma que solo usuarios conocidos puedan interactuar con el servidor.

Para entender la jerarquía de llamadas del sistema, se debe explicar la estructura del contrato que facilita el control de acceso. Cada usuario en el sistema se empareja a una dirección privada en la blockchain. Cada dirección privada está autorizada únicamente a hablar directamente con UN contrato en la blockchain. Este contrato es el contrato de clase individual. Instituciones, empleados de instituciones y clientes, son objetos de nivel de clase.

Estos objetos con nivel de clase son interfaces basadas en permisos. El Contrato Institucional tiene una lista de todos los clientes que tienen privilegios de visualización a la institución y cada contrato de cliente tiene una lista de instituciones a quienes ha dado el permiso. El contrato que tiene la institución tiene funciones que facilitan la revocación de permisos a la institución, por parte del usuario. El Contrato Institucional no puede alterar esa lista, previniendo así el

acceso sin autorización a los registros individuales. Adicionalmente, el Contrato Institucional posee una lista de empleados autorizados la cual puede actualizar. .Este esquema de permisos debería idealmente funcionar de tal manera que la revocación automática de un permiso se realice en intervalos semi-regulares para prevenir que una institución mantenga por error los permisos de acceso a información de antiguos empleados.

Dentro de este sistema, todos los participantes externos interactúan por medio del envío de una transacción firmada que codifica la llamada de la solicitud. Estas transacciones son enviadas por el servidor RPC luego de la validación del usuario. El servidor RPC envía las solicitudes al servidor de acumulación de datos, quien después los reenvía a los mineros basados en un mecanismo de distribución de cargas. Los mineros entonces procesan la solicitud enviando la transacción a nombre del solicitante hacia su respectivo contrato controlador. Este contrato contiene los permisos de los datos que la entidad tiene autorización de acceder dentro del contrato. Este contrato es la única entidad que aceptará una transacción desde una solicitud externa. Por tanto, un mecanismo es establecido para controlar el llamado a operaciones dentro de la blockchain.

Para cada transacción, se crea un registro inmodificable de quién hace el llamado. Esto asegura que todos los intentos de acceso de información queden registrados. Los datos grabados dentro del contrato del usuario son un sistema de punteros hash que, cuando son resueltos por el sistema de almacenamiento HIPAA, resultan en el retorno de los datos correctos. Esta información se eleva hacia el redireccionador HIPAA por medio de la ejecución de una transacción de solicitud válida. El mecanismo que facilita esta comunicación es indirecto y se manifiesta por medio del sistema de mensajería de eventos de la blockchain. Dada la limitación que el solicitante puede únicamente consultar la base de datos por medio de una transacción válida, y que el usuario no puede directamente alterar su propia información, el control de acceso es demostrable. Desde la perspectiva de las instituciones, el mecanismo es similar, excepto que el Contrato Institucional alberga una lista de usuarios de los cuales puede solicitar datos y una lista de usuarios que pueden interactuar con esta institución como empleados. Cuando una transacción solicitante se origina desde el contrato de un empleado de la institución, el contrato controlador llama el contrato institucional, quien llama el contrato de usuario para preguntar por los punteros a los datos que devuelven los ePHI. Si se asume que la institución está en la lista de instituciones aprobada por el usuario, el contrato retorna los punteros apropiados. Estos punteros son luego publicados como un evento de mensaje que, de nuevo, sube hasta el sistema de almacenamiento HIPAA.

Para claridad, el proceso completo de una solicitud única es así: El solicitante externo pide datos al servicio por medio de una llamada al servidor RPC con una transacción firmada criptográficamente. El servidor RPC verifica la identidad de la entidad externa por medio de la firma de la solicitud de ingreso

Si se verifica que la firma concuerda con una entrada en la base de datos de llaves públicas con permisos, el servidor RPC acepta la solicitud y envía la petición a los verificadores privados de la blockchain. El verificador ejecuta este llamado y en el evento que esta solicitud es una acción

permitida, la transacción se ingresa en el siguiente bloque. Esta transacción también causa la emisión de un evento de mensaje en la blockchain. Este evento mensaje es observado por el Redireccionador HIPAA, quien actúa con la creación de un mensaje cifrado para el Almacén de datos HIPAA basado en los hash del evento de mensaje. Este mensaje también contiene la llave pública del solicitante. La base de datos HIPAA observa esta solicitud y transmite una copia cifrada de la información al servidor RPC usando la llave pública del solicitante. El servidor RPC luego retorna esta información al solicitante mapeando la IP solicitante a la llave pública en el mensaje. El servidor RPC transmite este mensaje sin ver nunca los datos subyacentes. Estos datos son inmediatamente destruidos por el servidor RPC, asegurando así que el servidor RPC actúe como un conducto que no necesita cumplir con los requerimientos HIPAA.

El mecanismo para publicar datos es, de nuevo, de naturaleza similar, pero los datos que se envían se cifran con la llave pública del Almacenamiento HIPAA. Las otras operaciones son idénticas, excepto que los datos que se están enviando van subiendo por el sistema de mensaje de eventos. Así, dado el uso de funciones de hash de baja colisión y nonces con marca de tiempo, los datos pueden ser guardados y el contrato es capaz de calcular la dirección donde los datos enviados pueden ser localizados en el Almacén HIPAA.

Finalmente, se debe tratar la distribución de llaves privadas. Esta puede ser facilitada por medios ópticos para usuarios de teléfonos inteligentes. Esto sería análogo al uso de códigos QR como direcciones para Ethereum. Otros medios pueden también ser establecidos por aplicaciones tanto en equipos de escritorio así como tablets o teléfonos inteligentes. La pérdida de una llave no es un evento catastrófico, dada la habilidad administrativa de remover el control de acceso a un contrato para una llave y asignárselo a otra.

Interoperabilidad

Los sistemas EHR están basados en una arquitectura separada de validación de credenciales, en el que los datos del paciente se mantienen en cada uno de los sistemas de forma separada. Esto ha resultado en software de coordinación uno-a-uno con soluciones "add-on" para estos sistemas que les permiten la coordinación del cuidado del paciente con otros proveedores y organizaciones auxiliares de salud. Sin embargo, el acceso a la información desde la organización principal proveedora hacia las otras organizaciones es únicamente por medio de una capacidad limitada, como en los casos de Leer, Enviar, Transmitir o Notificar. Más aún, el Paciente o Consumidor tiene muy limitada su interacción o involucramiento en este intercambio de información. En adición, un problema con los mecanismos existentes de intercambio de datos es la dificultad en la rectificación de errores que puedan ocurrir durante el proceso de envío.

Una vez que se configure una blockchain y sus contratos inteligentes, los parámetros se vuelven absolutos. El paciente se vuelve el intermediario principal en el envío y la recepción de información de salud, negando la necesidad de actualizaciones frecuentes y análisis de problemas de cualquier software. Dado que los registros blockchain también son imposibles de modificar y se guardan a través de todos los participantes, contingencias de recuperación son innecesarias. Aún más, la estructura transparente de información de la blockchain elimina muchos puntos de integración de intercambio de información y actividades de reporte que consumen mucho tiempo.

Procesos y Escalabilidad

Los usuarios están en control de toda su información y transferencias lo que asegura datos de alta calidad, completos, consistentes, a tiempo, precisos y disponibles, haciéndolos durables y confiables. Gracias a la base de datos descentralizada, blockchain no tiene un punto central de falla y está mejor equipada para resistir ataques maliciosos.

http://imgur.com/UfPkBTA

Diagrama de flujo de proceso Blockchain

En cualquier red de salud, es necesario asegurar que participantes que colaboren pueden confiar en que cada uno entrega los servicios necesarios que se esperan de ellos. Para lograrlo, tienen que existir medios para asegurar la responsabilidad de tareas y servicios que se espera sean entregados a tiempo y también la asociada penalización si no son entregados a tiempo, en la calidad esperada. Por tanto, cualquier infraestructura tiene que ser capaz de revisar la información sin inconvenientes, para permitir

al Proveedor Primario del servicio evaluar su red. Más aún, a medida que la red crece, estas interacciones entre proveedores de la red incrementa las necesidades de la infraestructura para ser capaz de manejar esta escala.

El aspecto principal para construir un sistema de gestión de salud altamente escalable y distribuido es con un marco de arquitectura punto-a-punto. Marcos similares han sido usados en varios segmentos de la industria como, medios, deportes, inmuebles, cadenas de proveedores, mostrando que blockchain puede fácilmente ser un conector "add-on" para estructuras centralizadas existentes [#7]. Esto nos ha llevado a explorar el uso de blockchain por su aplicabilidad para permitir un marco punto-a-punto para el sector Salud.

Blockchain mantiene la promesa de validar dos o más entidades participantes en una " transacción de salud". Esto provee dos atributos claves al comparar con el modelo de autenticación centralizado. El primero es que las partes interesadas pueden interactuar con los otros a un "nivel transaccional" de "relación de confianza". El segundo es que la exposición de la responsabilidad en una relación de este tipo se limita únicamente al compromiso a "nivel transaccional". Esto es muy útil ya que limita el acceso de información y responsabilidades entre partes involucradas y al mismo tiempo habilita a un participante a entrar en una relación transaccional con un variado número de proveedores basados en sus capacidades específicas y tipos de cuidado entregados al paciente. Esto es significativamente mejor que el sistema convencional centralizado que necesita limitar el número de proveedores para un gran número de necesidades de los pacientes, dado el esfuerzo requerido para administrar el acceso y las responsabilidades.

Intercambio de Información de Salud y Tokens

El token Patientory (PTOY) es el combustible que mantiene la infraestructura blockchain. El uso principal del token es la regulación de los recursos de almacenamiento de la red, las mediciones de calidad de la salud y los ciclos de pagos de ganancias.

A los pacientes se les asigna una cantidad de espacio para guardar información gratis en la red Patientory. PTOY les permite comprar espacio extra ubicado en nodos configurados en los sistemas de los hospitales. PTOY puede ser comprado en la plataforma o en un intercambio.

Las organizaciones de salud usan PTOY en este caso también. Se usa igualmente en pagos una vez que se ejecutan los contratos inteligentes con compañías de seguros de salud y sirve como mecanismo para regular las métricas del modelo basado en valor.

Para lograr que los EEUU cambien exitosamente de un modelo basado en pago-por-servicio al modelo basado en valor, tiene que existir una infraestructura que permita a las organizaciones vincular calidad, valor y eficacia de las intervenciones médicas a través de un modelo de compensación acreditado.

La compensación se basará en qué tan efectivo es el trabajo en conjunto de la red de proveedores en asegurarse que hay una mejora en la calidad del cuidado y en el bienestar del paciente, al mismo tiempo que se reduce el costo asociado al cuidado. Para incentivar verdaderamente a los diferentes participantes en la red a crear pro-activamente mejores regímenes de cuidado, una compensación

basada en méritos de los ahorros compartidos (reembolsos) debe aplicarse. Para lograr efectivamente separar una parte proporcionada al proveedor en la red que contribuyó mayormente hacia los ahorros en general, un seguimiento claro de su contribución es medible por medio de contratos inteligentes en la red blockchain.

Otro impacto clave del nuevo paradigma de salud es el modelo de compensación donde los proveedores son elegibles de recibir compensación adicional al cuidado entregado. Esta compensación es el resultado de los ahorros que son generados basados en qué tan efectivos son los proveedores en administrar el cuidado y los resultados de la salud del paciente (incentivos). Cualquier ahorro generado por la gestión efectiva del cuidado del paciente puede ser mantenida por los proveedores y su red de asociados como parte de los ahorros compartidos del nuevo paradigma de salud.

Nuestra propuesta posibilita la habilidad de los pagadores a transferir tokens como incentivos a los proveedores que logren esas métricas de calidad. La habilidad de verificar fácilmente y administrar contratos inteligentes en los que los beneficios pueden ser redimidos con facilidad significativa provee la necesaria "zanahoria" para que los proveedores y pacientes interactúen en una colaboración simbiótica. En forma contraria, si uno o más participantes falla, se pueden determinar con igual facilidad las penalidades apropiadas, por medio de las responsabilidades. Esta aproximación "zanahoria / palo" proveerá el empuje necesario para cambiar la industria de una mentalidad de gestión de la enfermedad a una mentalidad del control del bienestar.

Por esto, los tokens PTOY expedidos por Patientory, son el token nativo para usar en la plataforma Patientory. A cambio de los tokens PTOY, los usuarios serán capaces de usar la red para alquilar espacio de almacenamiento para información de salud, y para ejecutar pagos y transacciones de contratos inteligentes específicos.

Creemos firmemente que usar un token es el mejor sistema de pagos para soportar la infraestructura en el futuro visible. Este futuro es un vibrante ecosistema de muchos tokens, para los cuales el sistema de salud necesitará crear sistema de pagos cerrado. El resultado será un ciclo de retroalimentación positiva para la gestión eficiente del cuidado, con disminución significativa en los miles de millones de dólares atribuidos actualmente a pérdidas por fraude al sistema de salud[4]4.

El sistema también incentiva aquellas organizaciones grandes con capacidad de almacenamiento a cambiar tokens con organizaciones más pequeñas o medianas que van a necesitar acceso directo a la red blockchain sin implementar un nodo directamente. Aunque las políticas del nuevo sistema de salud proveen el potencial para incentivar a los proveedores a trabajar juntos para mejorar los métodos de cuidado del paciente, las arquitecturas actuales de EHR no pueden habilitar esta capacidad, por tanto, simplemente con la entrega o recepción de tokens se facilita este proceso.

Por esto, el valor de los tokens está atado al volumen de transacciones que se ejecuten en la red. A medida que la red de Patientory aumenta constantemente en transacciones de tokens, la demanda de tokens se incrementa, resultando en un valor incrementado.

http://imgur.com/9WW3GCs
Valor del Token Patientory en función de las transacciones

Adquisición de Tokens

PTOY puede ser adquirido a través de la aplicación nativa de Patientory, de un mercado de

criptomonedas y de otros pacientes, médicos o aseguradoras por medio de una transferencia. Los usuarios de la plataforma tendrán la habilidad de adquirir PTOY enviando Ether (ETH) al contrato de creación PTOY en la blockchain durante la pre-venta. La interfaz de Patientory se integrará con soluciones de terceros en el mercado como Shapeshift y Coinbase para los usuarios que no tiene ETH.

Las distribuciones iniciales de Tokens Patientory ser harán en forma de pre-venta. Cualquier persona podrá adquirir PTOY a una tarifa con descuento enviando ETH al contrato inteligente de compra de tokens. Aquellos con otras criptomonedas como ETC o BTC pueden crear PTOY por medio de un servicio de un tercero de conversión que estará disponible en la página de pre venta.

El equipo fundador recibirá una asignación de 10% de PTOY, sujeto a un periodo de retención de 12 meses. Estos tokens servirán como incentivo a largo plazo para el equipo fundador de Patientory. Un 20% adicional se asignarán al fondo de la Fundación Patientory para ser usados en investigación y desarrollo en tecnología blockchain para casos de uso en la salud.

Contratos Inteligentes y procesamiento de reclamaciones de seguros

Auto-adjudicación

La complejidad de los procesos de facturación médica y reembolsos de terceros a menudo lleva a confusiones y malentendidos entre paciente, proveedor médico y asegurador. Estas complicaciones llevan a algunos consumidores a no tener claro cuándo, de quién o por cual cantidad ellos tienen que pagar una factura médica, o siquiera si el pago es su responsabilidad o del proveedor de seguros.

Patientory es una plataforma diseñada para aprovechar tanto las tecnologías blockchain de

Ethereum y las interfaces de aplicación (API) compatibles con los Recursos Interoperables Rápidos de Salud (Fast Healthcare Interoperability Resources, FHIR), para incrementar eficiencias, permitir adjudicaciones de reclamaciones en tiempo casi-real, proveer acuerdos transparentes entre participantes y disminuir fraudes.

FHIR se creó en la industria como un formato de datos estándar para reducir la complejidad de integración para sistemas existentes de salud y seguros. Un aspecto clave de nuestra solución, dado el costo de adicionar datos a la blockchain, es limitar esos datos a únicamente lo necesario para que se puedan ejecutar los contratos inteligentes.

Con costos relacionados con facturación y aseguramiento que se espera alcancen 315 mil millones de dólares (USD) en 2018, y oficinas médicas gastando 3.8 horas cada semana interactuando con pagadores, nuestra plataforma puede brindar una descarga sustancial de estos costos operacionales.

Métodos que se usan para el análisis de la correlación cruzada De información diagnóstica pueden ser también usados para analizar datos de reclamaciones por actividad fraudulenta. Este análisis también puede revelar acciones como comportamientos de búsqueda de drogas al presentarse múltiples instancias de reclamaciones. Ambos casos de uso añaden proposiciones de valor para el uso de este sistema por parte de las compañías de seguros, pero el beneficio último está fuera del alcance de esta información.

Debido al sistema basado en reglas que se ejecutan con los contratos inteligentes, los acuerdos de cobertura completa pueden ser codificados en contratos inteligentes que sean referenciados contra usuarios finales. Esto permitiría a una entidad médica preguntarle al sistema que verifique la existencia de cobertura, previo a la entrega del servicio. El uso del sistema para almacenar información de costos también permite la facturación automática entre instituciones e individuos como una deuda basada en tokens. Por tanto, una institución y un individuo pueden conocer los costos que están incurriendo. Esto remueve trabajo de los departamentos de contabilidad, añadiendo valor a la adopción del sistema.

Por esta razón, Patientory es un sistema de pagos cerrado. Se espera que la conexión entre cadenas pueda incluso permitir un intercambio seguro de valor a través de la blockchain pública de Ethereum. Este mecanismo ya está resuelto para la arbitración de transacciones Bitcoin, aunque requiere una entidad confiable para actuar como Oráculo

Factibilidad

A través de mecanismos existentes, esta arquitectura ya puede ser construída. Un ejemplo sería la vinculación del sistema de almacenamiento HIPAA ofrecido por Amazon Web Services, con la plataforma ErisDB. Este Software como Servicio (Service as a Software, SAAS) permite la implementación rápida de una blockchain capaz de ejecutar contratos inteligentes Ethereum con control de accesos completamente regulados como los mencionados anteriormente. La adición de nodos pasivos debería ser construída, pero esto requiere un costo de desarrollo mínimo comparado al desarrollo de una arquitectura completa.

Con la arquitectura de contratos inteligentes de tres capas de Patientory, solo un subconjunto de características de los contratos inteligentes son implementados en la blockchain de Ethereum. La compleja lógica de negocio se remueve del camino de la ejecución, lo que

permite a la capa de datos ser optimizada para reflejar la naturaleza distribuida de la red.

Los componentes de los paquetes de contratos inteligentes implementados en la blockchain ethereum son el esquema de base de datos, transacciones de validación y verificación que añaden o modifican el libro, y la optimización de lógica de búsquedas para la lectura del libro.

La lógica de negocios se ubica encima de la blockchain ethereum en una capa media de negocios. Este código implementa la lógica de una variedad de servicios, incluyendo ejecución segura, garantías, identidad, soporte criptográfico, formato de datos, mensajería confiable, disparadores y la habilidad de conectar dicho código con el esquema en contratos inteligentes específicos en cualquier número de blockchains, permitiendo a Patientory conectarse a varios consorcios de salud. Estos servicios se proveen en una capa, donde las partes de código individuales que soportan los contratos inteligentes pueden ejecutarse, enviar transacciones a los nodos de la blockchain, y conectarse al esquema en la base de datos.

Beneficios únicos adicionales

Aunque una institución médica, como un hospital, no debería tener acceso a ningún registro que no hayan sido específicamente autorizado, al tener usuarios con una pre-autorización para compartir información bajo situaciones de emergencia, el usuario final podría obtener beneficios adicionales por su participación en el servicio. Con esto en mente, la necesidad de una institución médica de acceder a los registros de una persona que no responde en situaciones de emergencia constituye una situación que amerita el el escalamiento de los privilegios, si se da que el usuario haya autorizado previamente este acceso. En el evento que una persona no responde, y tiene su teléfono celular presente, la

institución puede probar la posesión del dispositivo del individuo utilizando un método de firma secundaria que está disponible en la pantalla de bloqueo del teléfono. Esta segunda clave no debe ser la misma llave privada principal de la cuenta. Por tanto, si la cuenta de una institución envía una solicitud a la blockchain conteniendo la clave pública de un individuo y el teléfono de dicho individuo ha enviado la clave de emergencia, la blockchain puede escalar privilegios para permitir acceso a los registros por parte del personal médico que de otro modo no tendría acceso.

Esta clave privada debe considerarse temporal y ser reemplazada por el individuo tan pronto como sea posible. En esta forma, el intercambio seguro de información entre el individuo y una institución autorizada puede facilitarse en condiciones de emergencia

Si una institución solicita esta información sin la autorización apropiada, el individuo sería notificado de estas acciones. Si el individuo niega la solicitud dentro de un intervalo de tiempo, los datos no son compartidos. Más aún, si una institución intenta múltiples solicitudes fraudulentas, la institución puede ser castigada con una revocación de privilegios, castigos monetarios y/o acciones legales. El daño causado por la pérdida de un celular es mínimo dada la necesidad de tener dos claves, la del teléfono y la de la institución. En el futuro visible, todas las tarjetas de aseguradoras podrían tener incluidos micro controladores criptográficos, iguales a los de las tarjetas de crédito modernas, que facilitarían la misma operación independientemente del teléfono.

Prioridades de salud Nacionales / Internacionales

Cuidado personalizado

Para lograr un cuidado efectivamente superior, un acercamiento centrado en la persona es importante. Este acercamiento debe tomar en cuenta no solo los aspectos clínicos sino

también los factores económicos y sociales que impiden la habilidad de la persona para vincularse exitosamente en el cumplimiento de sus cuidados y el estilo de vida saludable que lleva a un bienestar sostenido.

Para obtener resultados efectivos del cuidado se requiere identificar claramente las barreras de la salud individual y sus situaciones de vida. Con un número creciente de pacientes con presencia de 2 o más comorbilidades, la aproximación "centralizada" donde un tipo de tratamiento sirve para todos, no conduce en la motivación y guía efectiva para obtener resultados de los cuidados. Por tanto, un modelo de cuidado más flexible, personalizado para incluir las características de salud y bienestar polifacéticos de un paciente, tienen que ser considerados. Esto requiere de un plan de cuidado que sea comprensivo, dinámico e interactivo en el que sea vital que el paciente pueda seguir, gestionar y participar en el cuidado del individuo.

Resultados clínicos

Las Mediciones de Resultados Relacionadas al Paciente (Patient-related outcome measures, PROM), que se enfocan en los resultados que están directamente relacionados con el paciente, han tenido importancia adicional y significado en los últimos años. Esto se debe, en parte, al incremento de la atención enfocada en la experiencia del paciente durante el cuidado y para proveer una revisión enfocada en el paciente sobre la carga y el impacto de la enfermedad. Los PROM pueden incluir síntomas y otros aspectos de salud relacionados con indicadores de la calidad de vida como función física o social, adherencia al tratamiento y satisfacción con el tratamiento. Ellos también facilitan una comunicación más precisa entre el paciente y el médico en términos de la carga de enfermedades relacionadas con el tratamiento, al proveer una evaluación más completa y detallada de los tratamientos para condiciones específicas, como cáncer o esclerosis múltiple.

Los PROM son diferentes a otras mediciones de eficacia clínica tradicionales (por ejemplo, sobre vivencia al cáncer, eliminación del hábito de fumar) porque ellos directamente reflejan el impacto de la enfermedad y del tratamiento desde las perspectiva del paciente. Estas medidas pueden examinar el balance entre la eficiencia del tratamiento y su carga en el paciente. También es efectiva en la búsqueda de áreas como el funcionamiento físico y bienestar general, así como en resaltar la eficacia y seguridad de tratamientos en relación a su beneficio clínico en general. Porque estas mediciones por sí mismas son desarrolladas desde la perspectiva del paciente, también pueden facilitar un mayor involucramiento del paciente en las decisiones sobre el tratamiento así como proveer una guía para decisiones de salud general. Esencialmente, reforzando una blockchain con PROM se refuerza la habilidad de incentivar a proveedores y pagadores a cumplir con estándares de cuidado de la salud.

Conclusión

Blockchain jugará un rol cada vez más significativo en la infraestructura tecnológica de la salud y traerá cambios benéficos y nuevas eficiencias a para participante en el ecosistema. Es de vital importancia que las organizaciones de salud entiendan el corazón de la tecnología blockchain para asegurarse que están listos para los cambios que la tecnología conlleva.

El resultado será una nueva generación de poderosas aplicaciones basadas en blockchain que definirán la siguiente era de negocios en la salud. Para que blockchain llene su potencial en salud, debe estar basado en estándares para asegurar la compatibilidad e interoperabilidad dentro del panorama del sistema de salud centralizado.

Referencias

: Vitalik Buterin. “A next-generation smart contract and decentralized application platform.

White Paper". In: (2014.).

: Yan-Cheng Chang and Michael Mitzenmacher. "Privacy preserving key- word searches on remote encrypted data.In International Conference on Applied Cryptography and Network Security". In: ().

: Mayo Clinic. "Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014". In: (). url: www. mayoclinicproceedings.org.

: Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. "Reidao: Digitising Real Estate Ownership". In: (). url: http://reidao.io/whitepaper.pdf.

: Centers for Disease Control Prevention. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services." In: (2003.).

: Roy Thomas Fielding. "Architectural styles and the design of network-based software architectures." In: (2000.).

: HHS.gov. "H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule". In: (2013). url: www.hhs.gov/hipaa/for-professionals/ privacy/laws-regulations/index.html.[Accessed:04-Apr-2017].

: HHS.gov. “Methods for De-identification of PHI”. In: (2015). url: https://www.hhs.gov/hipaa/forprofessionals/privacy/specialtopics/de-identification/index.html#protected.[Accessed:04Apr-2017].

: Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. “Proof of activity: Extending bitcoin’s proof of work via proof of stake.” In: (2014).

: Sunny King and Scott Nadal. “PPCoin: Peer-to-peer crypto-currency with proof-of-stake.” In: (2012).

: Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

: Stean D Norberhuis. In: ().

: Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen and Ivor DSouza. “The NLM Value Set Authority Center. ” In: (2013.).

: Amit P Sheth. “Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In Interoperating Geographic Information Systems,” in: (1999.).

: Nick Szabo. “Formalizing and securing relationships on public networks.” In: (1997.).

: “US GPO. CFRx 164 security and privacy. 2008.” In: (). url: http://www.access.gpo.gov/nara/cfr/waisidx08/45cfr16408.html. Accessed:2016-08-06

- 1 Begoyan, A. An overview of interoperability standards for electronic health records; USA: Society for design and process science (2007).
- 2 Charles N Mead et al. “Data interchange standards in healthcare it computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap?” In: (2006.).
- 3 Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. “MedRec”. In: (2016). url: www.pubpub.org/pub/medrec. [Accessed: 05-Apr-2017].
- 4 National Healthcare Ant-Fraud Association. “The Challenge of Health Care Fraud”. In: (). url: https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.