BLOCKCHAIN™ IN HEALTHCARE TODAY

INVESTIGACIÓN ORIGINAL

Resolución de conflictos de privacidad para integrar historiales médicos personales y electrónicos en sistemas basados en blockchain

Aleksandr Kormiltsyn, MSc[1] ; Chibuzor Udokwu, PhD[2] ;Vimal Dwivedi, PhD[3] ; Alex Norta, PhD[4] ; Sanam Nisar, MSc[1]

[1]Departamento de Ciencias del Software, Universidad Tecnológica de Tallin, Tallin, Estonia; [2]Austrian Blockchain Centre Research, Viena, Austria; [3]School of Electronics, Electrical Engineering and Computer Science, Queens University Belfast, Belfast, Irlanda del Norte, Reino Unido; [4]Baltic Film, Media and Arts School, Universidad de Tallin, Estonia; Dymaxion OÜ, Tallin, Estonia.

Correspondencia: Aleksandr Kormiltsyn, Correo electrónico: Aleksandr.kormiltson@taltech.ee

Palabras clave: blockchain, gestión de conflictos, sanidad electrónica, sanidad preventiva, privacidad, contratos inteligentes

Resumen

La integración de los historiales médicos personales (PHR) y los historiales médicos electrónicos (EHR) facilita la prestación de nuevos servicios a particulares, investigadores y profesionales sanitarios. Al mismo tiempo, la integración de los datos sanitarios plantea complejidades derivadas de la heterogeneidad estructural y semántica de los datos. El tema de los datos sanitarios suscita fuertes emociones debido a la preocupación que suscita la violación de la privacidad. La tecnología blockchain se emplea para abordar la cuestión de la privacidad de los datos de los pacientes en los procesos interorganizativos, ya que facilita la propiedad de los datos de los pacientes y promueve la transparencia en su uso. Al mismo tiempo, la tecnología blockchain crea nuevos retos para los sistemas de sanidad electrónica, como la privacidad de los datos, la observabilidad y la aplicabilidad en línea. Este artículo propone diseñar y formalizar técnicas automáticas de resolución de conflictos en sistemas sanitarios electrónicos descentralizados. El presente estudio expone nuestros conceptos empleando un caso práctico centrado en los ámbitos de la atención sanitaria preventiva y personalizada.

Resumen en lenguaje sencillo

Este documento sugiere el uso de la tecnología blockchain para los problemas de privacidad en la integración de los historiales médicos personales y los historiales médicos electrónicos en los sistemas descentralizados de atención sanitaria electrónica. Este informe se centra en el diseño de técnicas automáticas de resolución de conflictos para garantizar la propiedad de los datos de los pacientes, la transparencia y la privacidad en los procesos inter-organizacionales. Este artículo propone el diseño de técnicas automáticas de resolución de conflictos en sistemas sanitarios electrónicos descentralizados, que pueden mejorar los procesos interorganizativos en la atención sanitaria. El uso de la tecnología blockchain para integrar las historias clínicas personales y electrónicas puede garantizar la propiedad de los datos de los pacientes y promover la transparencia en el uso de los datos, abordando los problemas de privacidad en los sistemas sanitarios. Este artículo hace hincapié en la importancia de la privacidad y la protección de datos en los sistemas sanitarios, destacando la necesidad de cumplir las leyes y normativas. Los resultados de la investigación, incluido el prototipo de prueba de concepto, pueden aportar ideas prácticas para aplicar técnicas de resolución de conflictos en sistemas sanitarios electrónicos descentralizados.

Enviado: 26 de junio de 2023; Aceptado: 13 de noviembre de 2023; Publicado: 14 de diciembre de 2023

Hos sistemas sanitarios se ven afectados por los elevados costes[1]y los intereses económicos de los proveedores de servicios sanitarios. Por ejemplo, tras la privatización, el sector hospitalario irlandés se enfrentó a un aumento del número de camas de pacientes en los hospitales privados con ánimo de lucro, mientras que en los hospitales sin ánimo de lucro este número disminuyó[2]Una historia clínica personal (HCP) es la información electrónica relacionada con la salud de una persona. Se gestiona y La persona es quien controla el acceso a los datos. El PHR almacena y organiza el historial médico, los tratamientos, los medicamentos, las notas, los diagnósticos y otra información sanitaria relevante, que puede ser compartida entre el individuo y sus proveedores sanitarios. Los PHR ofrecen una relación completa y organizada del historial médico de una persona, lo que puede ser muy valioso para una consulta rápida y sencilla.

diagnóstico eficaz, mayor seguridad y calidad de la asistencia. Además, los PHR pueden utilizarse para hacer un seguimiento de la historia clínica de un paciente, identificar tendencias y correlaciones, y proporcionar información al paciente sobre sus proveedores de atención sanitaria.

Un circuito de retroalimentación en sanidad es un proceso en el que la información sobre el estado de salud de un paciente o el rendimiento de un sistema sanitario se recopila, analiza y utiliza para introducir mejoras o ajustes en la atención al paciente o en los procesos sanitarios. Un bucle de retroalimentación implica el intercambio de información sobre el estado del paciente, sus opciones de tratamiento y su evolución. Los pacientes informan sobre sus síntomas y experiencias terapéuticas, lo que ayuda a los profesionales sanitarios a tomar decisiones informadas sobre su tratamiento.

Las investigaciones definen el valor de los RPS como la mejora de la comunicación entre el paciente y el médico, lo que se traduce en una educación del paciente que conduce a cambios en su estilo de vida[3].La participación del paciente simplifica la recopilación y el procesamiento de datos personales sobre salud y bienestar, lo que aumenta el valor de los servicios sanitarios preventivos personalizados[4].Según Kormiltsyn y sus colegas[5],se prevé que surja una nueva clasificación de entrenadores sanitarios preventivos personalizados. Estos entrenadores utilizarán su experiencia y competencia en la comprensión y el análisis de datos sobre salud y bienestar. En nuestro artículo académico publicado en 2019, dilucidamos los predicamentos económicos y financieros del sistema sanitario y analizamos el potencial de la tecnología blockchain para facilitar sistemas descentralizados y orientados al paciente[6]En un sistema centrado en el paciente, los individuos son responsables de generar y administrar sus datos, mientras que los proveedores sanitarios emplean estos datos en sus procedimientos en lugar de poseerlos. Norta y sus colegas ilustran la cuestión del intercambio transparente de datos[7]

La recopilación y el tratamiento de los datos de los RPS plantean numerosos retos jurídicos, técnicos y emocionales. Los estudiosos se centran en los requisitos técnicos y de seguridad de los sistemas de PHR cuando los datos se gestionan de forma centralizada[8-10].Esta metodología resulta eficaz en situaciones en las que el número de fuentes de datos de PHR es limitado. De este modo, aumenta el número de procesos que utilizan el PHR y la necesidad de una mayor confianza entre las partes interesadas, como empresas privadas, instituciones jurídicas e individuos, y aumenta la complejidad de la integración. Por lo tanto, un enfoque centralizado no es escalable, mientras que los procesos inter-organizacionales descentralizados basados en la tecnología blockchain proporcionan una base para conexiones fiables y escalables.

Un sistema integrado de PHR y de historia clínica electrónica (HCE) es sociotécnico e implica a personas de distintas organizaciones que utilizan diferentes conjuntos de tecnologías para colaborar y resolver problemas[11]. Una HCE son los datos de un paciente creados por profesionales sanitarios y almacenados digitalmente. Estos datos incluyen el historial médico, la medicación, el estado de inmunización, los resultados de las pruebas de laboratorio y las imágenes radiológicas. La HCE permite a los profesionales sanitarios planificar y prestar una atención personalizada al paciente de forma eficaz y segura.

compartir información médica entre profesionales sanitarios y otros usuarios autorizados. Además, las HCE pueden ayudar a reducir los costes sanitarios y mejorar la calidad de la atención. La decisión de utilizar un sistema centrado en el paciente que comparte la HCE está motivada emocionalmente y crea una sensación de incertidumbre sobre la forma en que se utilizan los datos personales.

El uso de PHR integrados en la HCE crea conflictos de seguridad, protección de datos y privacidad. La privacidad es un término jurídico que limita el conocimiento y el control sobre el contenido y la ejecución de un contrato (inteligente), que sólo debe distribuirse entre las partes en la medida necesaria.[12]Mientras que la privacidad, tal como se define en la Carta de los Derechos Fundamentales de l a Unión Europea,[13]es el derecho de toda persona a que se respete su vida privada y familiar, su domicilio y su correspondencia,[7]) la protección de datos se refiere específicamente al tratamiento de datos personales y está orientada a salvaguardar esta privacidad.[8]La Carta hace hincapié en que los datos personales deben tratarse de forma leal, con fines concretos y basándose en el consentimiento de la persona afectada o en algún otro fundamento legítimo establecido por la ley. Esta distinción es crucial en nuestra investigación, ya que subraya la importancia de aplicar sistemas basados en cadenas de bloques de manera que se respeten tanto los derechos a la intimidad como los principios de protección de datos establecidos en la estos derechos fundamentales.

La norma, definida por la Comisión Europea (CE), propone cláusulas contractuales de la Unión Europea aprobadas por la UE en junio de 2021[14].Es importante señalar que estas cláusulas debían ser sustituidas por versiones actualizadas en diciembre de 2022 como parte de los esfuerzos continuos de la CE para mejorar las normas de protección de datos en consonancia con la evolución del panorama jurídico y tecnológico. Como se indica en la documentación de la CE sobre las cláusulas contractuales tipo, esta actualización es un paso importante para garantizar unas medidas de protección de datos sólidas y actualizadas en las transferencias transfronterizas de datos.

En 2010 Proceedings of the 2010 IEEE 3rd Interna-tional Conference on Cloud Computing,[15]la Junta Europea de Protección de Datos (JEPD) y la Autoridad Española de Protección de Datos (AEPD) aclaran que cuando los identificadores están vinculados a un hash, como un número de teléfono, la información puede ser inequívocamente rastreada hasta un titular de datos específico. Esta vinculación introduce vulnerabilidades adicionales a la confidencialidad del hash, ya que el identificador vinculado puede reducir potencialmente el espacio de mensaje efectivo para ese hash en particular, comprometiendo así su función de seudonimización prevista. Esta idea pone de relieve las posibles limitaciones y dificultades de la utilización de funciones hash para la protección de datos, y subraya la necesidad de considerar cuidadosamente su aplicación en sistemas basados en cadenas de bloques.

Sun y sus colegas[16]definen los principales requisitos de los sistemas médicos que emplean el Internet de las cosas (IoT) como la integridad de los datos, la facilidad de uso, la auditoría y la seguridad del paciente.

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

privacidad de la información. Al-Muhtadi y colegas[17]se centran en los problemas de ciberseguridad y privacidad al integrar aplicaciones sanitarias móviles y proponen una arquitectura segura para entornos multicloud. La investigación de Katurura y Cilliers[18]afirma que los usuarios carecen de control y transparencia de los datos. Además, los investigadores han descubierto un desconocimiento de los riesgos para la seguridad y la privacidad relacionados con los datos personales de los dispositivos vestibles[(19).]Varios autores han destacado que compartir datos médicos conlleva riesgos para la seguridad y la privacidad[20-22].Simultáneamente, los autores afirman la necesidad de seguir investigando para desarrollar sistemas sanitarios seguros e integrados. La recogida autónoma de datos sanitarios plantea nuevos retos para la privacidad de los datos cuando se utilizan sistemas domésticos inteligentes[(23-25).]

Salehi y Giacalone propusieron el uso de algoritmos equitativos para resolver conflictos civiles[26,] basados en distintas tecnologías, como la inteligencia artificial (IA) y los sistemas algorítmicos de decisión (SDA). En su publicación[(27).]Xu y sus colegas presentan una investigación sistemática que emplea el Modelo Gráfico para la Resolución de Conflictos (GMCR) como enfoque viable para abordar conflictos del mundo real. Otros estudiosos[28]utilizan modelos ocultos de Markov (HMM) para escudriñar los datos entrantes y conciliar los conflictos que puedan surgir. El análisis incluye la cus-tomización y el entrenamiento de los modelos HMM, que posteriormente se utilizan con un sistema basado en reglas para detectar información conflictiva, resolver los conflictos identificados y utilizar datos y decisiones anteriores para prevenir conflictos antes de que se produzcan. Algunos investigadores[29]sugieren utilizar un mediador que detecte los conflictos y ofrezca una posible solución a las partes en conflicto.

La pregunta principal de la investigación es cómo resolver automáticamente los conflictos en los procesos interorganizativos integrados de asistencia sanitaria electrónica. Para responder a la pregunta principal de la investigación, deducimos las siguientes subpreguntas. ¿Cuáles son los requisitos para la recopilación y el procesamiento interinstitucional de los RPS centrados en el individuo? La respuesta a esta pregunta pretende definir el espacio lógico de requisitos que incluye las asignaciones de las partes interesadas. ¿Qué conflictos surgen en los procesos interorganizativos de atención sanitaria electrónica? Para responder a esta pregunta, se definen los conflictos que surgen en los procesos interinstitucionales de atención sanitaria electrónica y se alinean con los procesos descritos en la pregunta de investigación anterior. Además, estos procesos se diseñan utilizando el Modelo y Notación de Procesos de Negocio (BPMN). ¿Cuáles son las técnicas de resolución automática de conflictos en la sanidad electrónica descentralizada? El objetivo de la técnica de resolución de conflictos de privacidad es crear un proceso de resolución de conflictos para la sanidad electrónica, utilizando BPMN, basado en el diseño del proceso en el que surgen los conflictos, tal y como se define en la investigación anterior.
investigación.

A continuación se presenta un resumen del resto de esta revisión.

- Una revisión de la literatura, preliminares y un caso práctico.
- Discusión de los requisitos de recopilación y procesamiento de PHR centrados en el paciente.
- Presentación de los conflictos en el proceso descentralizado de la sanidad electrónica, relacionándolos con objetivos funcionales y procesos empresariales específicos.
- Abordar las técnicas de resolución de conflictos de privacidad al procesar datos médicos en procesos interorganizativos.
- Evaluación del proceso ideado y yuxtaposición de los resultados con los de otras investigaciones.
- Conclusión en la que se exponen las limitaciones, las cuestiones sin resolver y las posibles vías de investigación futura.

Revisión bibliográfica y preliminares

A continuación, los autores revisan la bibliografía relacionada y presentan los preliminares que esbozan los antecedentes de esta investigación.

Revisión bibliográfica

La investigación sobre la tecnología blockchain en la sanidad ha aumentado notablemente[30-32]. Las principales áreas de interés en este campo son el intercambio de datos, los historiales médicos y el control de acceso. Un libro de contabilidad distribuido, como el que propone una cadena de bloques, plantea el concepto de que los participantes añadan nuevos registros. La información almacenada en una cadena de bloques es inmutable, lo que se garantiza mediante criptografía[(33).]Los datos contenidos en la cadena de bloques se almacenan de forma segura en transacciones, que luego se organizan y enlazan en bloques mediante métodos criptográficos.

Cada bloque está intrincadamente conectado con el siguiente bloque de la cadena. La utilización de la técnica criptográfica conocida como árbol de Merkle, o árbol hash, garantiza que las transacciones almacenadas en una cadena de bloques estén correlacionadas mediante hashes matemáticos[34,35], asegurando así que ninguna alteración pueda invalidar la totalidad de los datos registrados. Los hash agilizan el proceso de validación de nuevas transacciones, obviando la necesidad de analizar toda la información almacenada en una cadena de bloques[(35)]Algunas cadenas de bloques, como Ethereum, admiten contratos inteligentes que los nodos pueden ejecutar.

Metodología de investigación

La investigación en ciencias del diseño (DSR) se utiliza en este documento para "llevar a cabo la investigación". La DSR ofrece un marco para desarrollar y evaluar nuevos artefactos[(36)]El entorno, la evaluación DSR y la base de conocimientos son los tres componentes principales de la DSR. El entorno de la investigación describe los problemas a los que se enfrentan las organizaciones y los ámbitos de aplicación. La base de conocimientos ofrece apoyo teórico para desarrollar nuevos artefactos que resuelvan los

problemas organizativos identificados. El artefacto creado se evalúa como parte de la DSR.[36]

La investigación previa de Narendra y colegas[11] realizada por los autores sobre el enfoque de resolución de conflictos en el entorno M2X (Machine-to-Everything) sirve como pilar del entorno para este estudio. En este artículo, el enfoque propuesto anteriormente se adapta a un entorno de sanidad electrónica en el que las partes implicadas en los procesos interorganizativos carecen de confianza.

La base de conocimientos representa las estrategias, técnicas y modelos existentes que sirven como bloques de construcción para diseñar los métodos de resolución de conflictos y el flujo de procesos interorganizativos descentralizados. Utilizamos el marco Trustable DApp Modeling (T-DM) para definir los requisitos del proceso de diseño, ya que amplía el enfoque Agent-Oriented Modeling (AOM) e introduce objetivos tokenizados utilizados en los sistemas blockchain. Remitimos al lector a "Preliminares" para una descripción más detallada del marco de gestión de datos de prueba (T-DM) y BPMN para definir los flujos de proceso.

Las técnicas de resolución automática de conflictos diseñadas se evalúan en los procesos descentralizados de atención sanitaria electrónica con el modelado de Redes de Petri Coloreadas (CPN). Además, proporcionamos un prototipo de prueba de concepto (PdC) que ilustra la implementación del caso en ejecución. El enfoque de evaluación es similar al utilizado en la investigación anterior.[11] Además, proporcionamos la implementación del caso de ejecución modelado con el PoC.

El caso práctico y los antecedentes previos

Para garantizar la confidencialidad y facilitar la resolución de conflictos, ofrecemos un análisis exhaustivo en la sección "Caso en curso y escenario del conflicto de privacidad", que presenta un escenario práctico desde un punto de vista centrado en el paciente. El presente caso práctico pretende facilitar la comprensión del caso en curso y de las secciones posteriores de este documento. La sección "Preliminares" ofrece la información introductoria necesaria para comprender los segmentos posteriores.

Caso en curso y escenario del conflicto de privacidad

La figura 2 presenta una descripción del caso en curso dentro del dominio de la prevención del cáncer. Mientras que los fisioterapeutas evalúan principalmente los resultados clínicos mediante la valoración del nivel de dolor, la amplitud de movimiento y la fuerza muscular, los dominios de los objetivos de los pacientes consisten en la actividad física, la calidad del entorno de trabajo y la calidad del sueño. La disparidad observada puede dilucidarse teniendo en cuenta la compleja naturaleza de la comparación de individuos mediante la Escala funcional específica del paciente (Pa-tient Specific Functional Scale)[37]. En nuestro caso, el paciente controla los datos sanitarios con un reloj inteligente y sensores de calidad del aire y del agua. Estos dispositivos Estos dispositivos recogen datos sobre la actividad, la salud y el entorno ecológico del paciente y los comparten si es necesario.

La información antes mencionada se recopila de forma continua, y el profesional sanitario recibe una retroalimentación durante el seguimiento del paciente. Además, cuando el paciente solicita atención médica a un médico generalista en un hospital, éste realiza pruebas de laboratorio, obtiene un historial médico y posteriormente incorpora estos datos a la HCE. En conclusión, tanto los profesionales sanitarios como los médicos generalistas acceden a la HCE en colaboración. Estas personas son responsables de presentar informes completos al proveedor de seguros para obtener el reembolso de las intervenciones médicas realizadas. Los informes médicos varían como consecuencia de la información a la que tiene acceso el profesional sanitario, que abarca el PHR junto con la aportación continua del paciente.

Este fenómeno aumenta la comprensión de las circunstancias relacionadas con la salud, lo que, a su vez, facilita la prestación de servicios sanitarios personalizados por parte del profesional sanitario. Por el contrario, el médico generalista se limita a acceder únicamente a la HCE debido a la falta de un mecanismo de retroalimentación.

La discrepancia a la hora de hacer valer la información médica con-tradice a la compañía de seguros, que carece de directrices para procesar los datos de la HCE. Tal disparidad complica aún más la utilización de los servicios sanitarios desarrollados recientemente que se basan en el procesamiento de PHR. Es plausible que la aplicación de un mecanismo de retroalimentación pueda mejorar la situación.

El paciente se enfrenta a conflictos de privacidad debido a la vulnerabilidad de sus datos en dispositivos autónomos inteligentes o en diversas aplicaciones, lo que provoca conflictos de privacidad. Una vez que el paciente proporciona su PHR al médico de atención primaria, después de que éste haya aceptado, con una explicación explícita, utilizar los datos del paciente con arreglo a los requisitos reglamentarios, este último puede emplearlos en los procedimientos internos del proveedor de asistencia sanitaria, por ejemplo, para generar informes, realizar análisis estadísticos y facilitar las tareas de investigación. Estos procedimientos pueden implicar a participantes externos, como la Oficina Nacional de Estadística, empresas de investigación independientes o empresas privadas especializadas en servicios de notificación de datos. La opacidad de los procesos para el paciente hace que no sean transparentes. En consecuencia, puede surgir la posibilidad de que se manejen mal los datos de los RPS.

En este artículo definimos tres conflictos durante el proceso de aseguramiento entre organizaciones. En primer lugar, la monitorización a domicilio entraña conflictos de privacidad cuando se recogen datos de los pacientes. Los dispositivos wearable y los sistemas PHR, que conservan los datos acumulados, son susceptibles d e que personas no autorizadas extraigan dicha información. A continuación, surge un conflicto de integridad cuando el PHR atraviesa varios procesos y es susceptible de ser alterado por las partes implicadas.

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

partes implicadas. Por último, el conflicto de consistencia surge cuando el proveedor de seguros recibe reclamaciones tanto del profesional sanitario como del médico, en las que proporcionan información disímil en la reclamación al seguro.

Preliminares

En este artículo se analizan los procesos de sanidad electrónica asociados a sistemas de cadena de bloques para lograr una trazabilidad inmutable, seguridad, desintermediación distribuida con garantía de privacidad y descentralización en la colaboración entre organizaciones. La tecnología blockchain proporciona un libro de contabilidad distribuido que permite a los participantes añadir y verificar registros en un libro de contabilidad, y la criptografía garantiza que los registros sean inmutables[33]. Cuando los participantes añaden registros al libro de contabilidad, se almacenan como transacciones hash y se agrupan en bloques. El vínculo criptográfico entre cada bloque y su procesador previo es una característica fundamental del sistema que nos ocupa. Los contratos inteligentes son programas ejecutables que se ejecutan y almacenan en la blockchain[38]. Según Nguyen y Kim[38] las plataformas de blockchain más comunes son Bitcoin,[39] Ethereum,[40] Hyperledger Fabric,[41] etc.

Las cadenas de bloques utilizan diferentes mecanismos de consenso para validar las transacciones. Por ejemplo, Bitcoin utiliza un algoritmo de consenso de prueba de trabajo (PoW). Este mecanismo asume que todos los nodos participantes están resolviendo un difícil problema matemático. Recompensa al primer nodo con el número de tokens permitiéndole añadir el siguiente bloque[38]. Ethereum utiliza un algoritmo proof-of-stake (PoS) en el que la validación no se basa en los recursos empleados en la resolución de problemas matemáticos, sino en la rep-utación de un nodo. Remitimos a nuestra investigación anterior[42] para más detalles sobre el uso práctico de la tecnología blockchain.

Para la tecnología blockchain, existen diferentes tipos de fichas. En este caso, proponemos utilizar dos tipos de tokens: tokens "ligados al alma" (SBT) utilitarios e intransferibles. La cuenta representa el "Alma", y los tokens en posesión de las cuentas como "Soulbound Tokens" (SBTs).[43]

El token de utilidad se integra en un protocolo existente en la blockchain y se utiliza para acceder a los servicios de dicho protocolo. Además, se utiliza como criptomoneda que representa el acceso a un producto o servicio. A diferencia de los tokens de utilidad, los SBT se definen por su singularidad y rareza. Este tipo de token proporciona la propiedad del token y las funciones de transferencia correspondientes. La utilización de SBT en el sistema descentralizado de atención sanitaria electrónica se sugiere debido a la necesidad de una gestión eficaz de la identidad y el control de acceso a los datos de atención sanitaria electrónica.

Para controlar el acceso a su gestión de identidades, los individuos necesitan la capacidad de gestionar no sólo sus identificadores, sino también los datos asociados a ellos. Este enfoque es fundamental para la identidad autosuficiente, que representa un cambio de los sistemas tradicionales de gestión de identidades a un modelo de administración de identidades impulsado por el usuario. En un modelo de este tipo, facilitado por la tecnología blockchain, los usuarios tienen pleno control sobre sus identificadores y los datos personales vinculados a ellos, lo que garantiza la protección de sus datos personales.

El ecosistema blockchain admite distintos tipos de participantes, como oráculos y Organizaciones Autónomas Descentralizadas (DAO). En el contexto de la cadena de bloques, los oráculos se utilizan para obtener datos externos que no están disponibles en la cadena de bloques. Los oráculos están centralizados y confían en el proveedor de datos externo, pero existe un problema conocido con los canales de recuperación de datos no seguros[40]. Sin embargo, los oráculos presentan problemas de fiabilidad y confianza.[45] Aunque los oráculos de prueba no pueden ser totalmente automáticos, esto da lugar a la intervención del agente para garantizar la corrección del comportamiento del oráculo. Caldarelli y Ellul[46] afirman que una DAO es una organización autónoma implementada con contratos inteligentes. El comportamiento y las reglas de negocio de la DAO están predefinidos con la lógica de los contratos inteligentes.

El sistema de atención sanitaria electrónica derivado se utiliza en una colaboración inter-organizacional basada en la externalización dinámica de servicios especificada en contratos electrónicos[47]. En la atención sanitaria, los procesos inter-organizacionales incluyen el intercambio de datos entre pacientes y proveedores de atención sanitaria u otras organizaciones como compañías de seguros. Este documento considera una perspectiva de sistema descentralizado y centrado en el paciente en el que los datos de los RPS fluyen a través de diferentes sistemas y están disponibles para agentes humanos y no humanos, como dispositivos inteligentes autónomos. Entre estos dispositivos se incluyen dispositivos portátiles que controlan la salud del paciente con sensores, componentes domésticos inteligentes, drones autónomos o incluso vehículos que participan en procesos sanitarios. La investigación de Grefen y sus colegas[48] presenta un marco conceptual para una pasarela de salud electrónica inteligente que adquiere y analiza la información médica recopilada. En nuestra investigación, integramos la estrategia de resolución de conflictos de privacidad propuesta en el artículo de Narendra et al.[11] en un ecosistema sanitario descentralizado, que engloba dispositivos inteligentes autónomos y su colaboración, como se describe en la Ref. 49.

En los sistemas sociotécnicos, el cumplimiento de las funciones sociales es fundamental[50]. Dado que estos sistemas no funcionan de forma autónoma, sino que son el resultado de la acción humana, la investigación propone un enfoque orientado a los agentes a la hora de modelar sistemas sociotécnicos complejos[51]. Como los actores simulados son similares a los humanos debido a su vinculación cognitiva y social con el conocimiento de sí mismos y la dependencia de su historia, un enfoque orientado a los agentes utiliza esto en el comportamiento de los agentes. En el ámbito de la cadena de bloques y los contratos inteligentes, el problema del oráculo se refiere principalmente a la confianza y fiabilidad que aportan los oráculos[45]. Como afirma Barr[52] este problema surge cuando los oráculos de prueba no pueden ejecutarse de forma totalmente automatizada. En el caso de que los oráculos no estén automatizados, la intervención de un agente se hace obligatoria para comprobar la veracidad del comportamiento observado. Consideramos los sistemas multiagente (MAS) y utilizamos un enfoque AOM[51] para definir los requisitos de

el proceso de integración de datos de PHR y EHR orientado a la privacidad.

El modelado de objetivos se utiliza para analizar dominios sociotécnicos[53], ya que los modelos de objetivos representan la propuesta de valor de un sistema. El valor del sistema está representado por objetivos funcionales y de calidad y por roles. El sistema requiere cierta capacidad o una posición representada por un rol para alcanzar sus objetivos. Un objetivo funcional representa el requisito funcional del sistema, y un objetivo de calidad representa un requisito no funcional o de calidad del sistema[53]. Los objetivos de calidad se denominan sinónimamente requisitos no funcionales en ingeniería de software[53]. Los objetivos funcionales, de calidad y emocionales son heredados por todos sus subobjetivos.

Dado que un sistema de sanidad electrónica centrado en el paciente es un sistema social impulsado más por el compromiso emocional que por la funcionalidad, la investigación[54]propone un Marco de Vinculación Emocional que incluye objetivos emocionales en la fase inicial del diseño. Este marco se integra en el marco T-DM. Lo amplía con objetivos emocionales que representan los sentimientos de emociones negativas de los usuarios, como la desconfianza y la falta de propiedad de datos privados y confidenciales[54]. La investigación de Kormilt-syn[55]define las emociones positivas y negativas a partir de la valoración de un producto o un servicio beneficioso o perjudicial. Mendoza y sus colegas[56]describen cómo los objetivos de calidad desencadenan diferentes emociones positivas y negativas entre los usuarios. Ejemplos de estos objetivos son la utilidad, la adaptabilidad y la facilidad de uso. En este artículo, situamos los objetivos emocionales entre un rol y un objetivo funcional para definir las emociones que influyen en los objetivos funcionales del sistema.

El tema de la gestión de la privacidad y la seguridad de los conflictos adquiere mayor importancia con el creciente uso de la IO, las redes sociales, etc. La investigación de Mendoza y sus colegas[57]define los conceptos básicos de la informática segura, afirman que la privacidad se centra en el gobierno de los datos de un individuo. Las medidas de seguridad se aplican para protegerse contra el acceso no autorizado, haciendo hincapié en fortalecer los datos contra diversas formas de ataques y prevenir el robo de datos[58].Varias publicaciones de investigación confirman la importancia de definir técnicas de gestión de conflictos cuando se comparten datos personales[59,60].

Para diseñar un modelo de objetivos para el sistema de e-salud descentralizado, utilizamos el enfoque definido en el marco de trabajo T-DM[61]que se centra en el diseño de aplicaciones descentralizadas (DApps) para apoyar los procesos inter-organizacionales. El marco T-DM amplía los diagramas de objetivos AOM[53,] [61]e introduce un nuevo concepto de objetivos tokenizados que representan los servicios descentralizados que realizan transacciones en la blockchain y gastan o ganan tokens. El enfoque basado en modelos del marco T-DM admite la asignación de modelos de objetivos AOM al modelo de arquitectura de componentes del Lenguaje Unificado de Modelado (UML).

Para evaluar la técnica de resolución de conflictos propuesta, diseñamos un modelo formal CPN[62]. CPN, un lenguaje de orientación gráfica, posee la capacidad de identificar posibles fallos de diseño, especificaciones ausentes y problemas de seguridad y privacidad en los sistemas. Sirve para diseñar, especificar, simular y verificar sistemas. Un modelo CPN es un grafo bipartito compuesto por fichas, lugares, arcos y transiciones. Los lugares tienen la capacidad de contener múltiples tokens con color, indicando atributos con valores correspondientes. Las transiciones en CPN se activan sólo cuando todos los lugares de entrada tienen los tokens requeridos en su lugar. Por último, las transiciones producen tokens que se adhieren a la condición en los lugares de salida[63]Nuestro modelo utiliza el lenguaje de programación CPN ML para simular el caso de ejecución descrito en la Figura 1. Research[63]proporciona información más detallada sobre CPN.

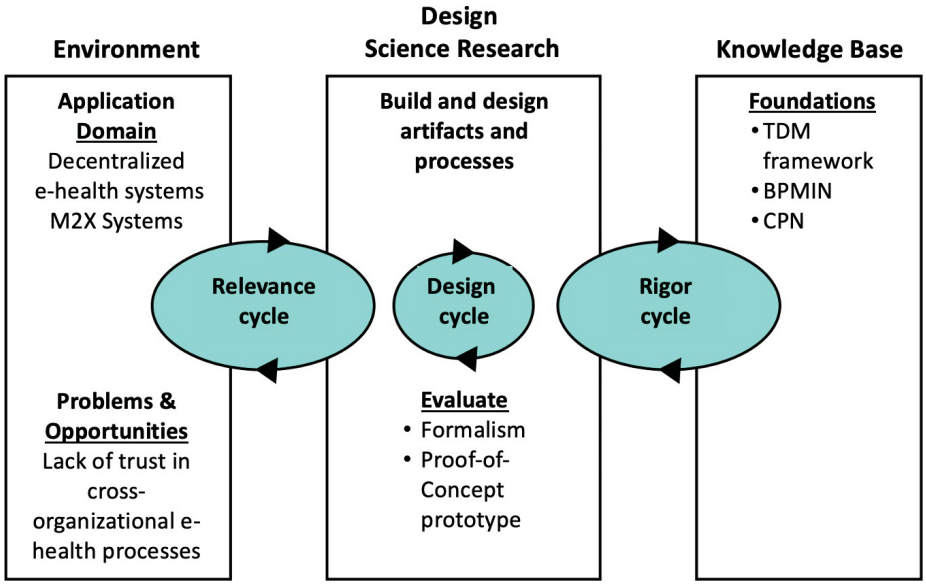

Fig. 1. Ciclos de investigación de la ciencia del diseño. BPMN: modelo y notación de procesos empresariales; CPN: Colored Petri nets; DSR: de-sign-science research; M2X: Machine-to-Everything; TDM: Trusted Document Management.

Citación: Blockchain en la sanidad hoy 2023, **6**: 276 - https://doi.org/10.30953/bhty.v6.276

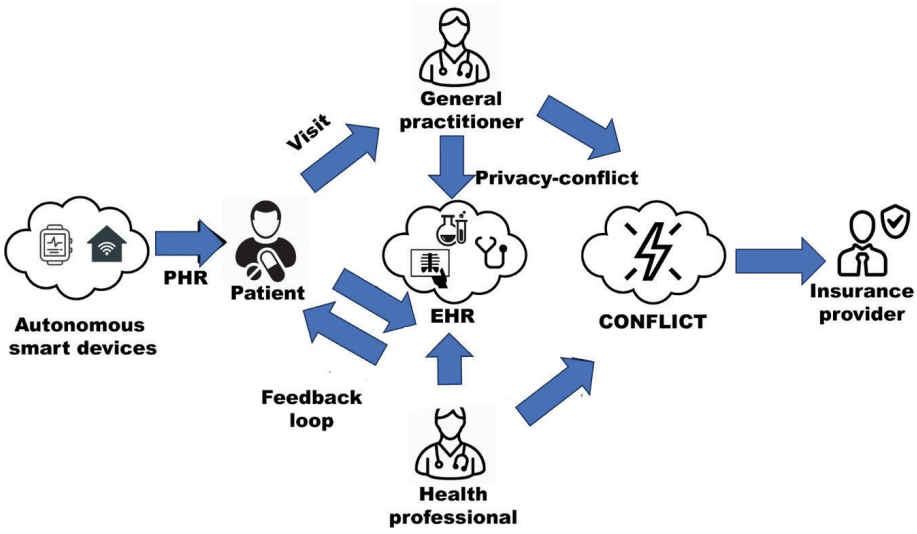

Fig. 2. Conflictos durante el procesamiento de los historiales médicos electrónicos (EHR) y los historiales médicos personales (PHR).

En un sistema de sanidad electrónica basado en blockchain, el intercambio de datos de confianza puede habilitarse mediante la autenticación multifactorial de identidad propia y soberana (MFSSIA)[64]para humanos y máquinas gestionada con tecnologías blockchain de contratos inteligentes.

La figura 3 ilustra cómo los usuarios humanos (nótese que también pueden ponerse dispositivos autónomos inteligentes en lugar de humanos) crean retos para otras entidades y les piden que respondan. O bien la entidad correspondiente no lo hace, o bien puede completar los retos con respuestas correctas. El reto elegido depende del caso de uso, el nivel de seguridad requerido y el nivel de amenaza de las entidades implicadas. En el ejemplo de la Figura 2, la identidad de la organización autentica un dispositivo autónomo proporcionando retos que el dispositivo debe realizar para confirmar su identidad. La organización decide si la respuesta satisface su solicitud. Ambos suben la solicitud y la respuesta a la cadena de bloques. En este caso, la autenticación falla si la entidad correspondiente no responde correctamente. En caso contrario la entidad se autentica correctamente.

La autenticación de identidad autosoberana multifactor challenge-set (MFSSIA) permite la interoperabilidad entre cadenas de bloques utilizando oráculos de cadena de bloques. Los oráculos son agentes digitales cuyo objetivo es obtener información del mundo exterior en una cadena de bloques. Los datos de diversas fuentes (monitores de presión arterial, PHR, EHR, etc.) se submiten a la blockchain como datos transaccionales.(64)Los oráculos se utilizan como fuentes de datos para que la información del mundo real sea consultada por contratos inteligentes que se ejecutan en blockchains y empujando datos a fuentes de datos desde la propia blockchain.[65]

Los conjuntos de retos en MFSSIA se almacenan en un grafo de conocimiento decen-tralizado (DKG[1]) . En el DKG, la información se almacena como un grafo de entidades y relaciones relevantes para un dominio u organización específicos. El DKG proporciona grafos inmutables, consultables y buscables que se utilizan en distintas aplicaciones.

[1]https://docs.origintrail.io/general/dkgintro

Resultados

La presente sección proporciona los resultados que constituyen las respuestas a las preguntas de investigación delineadas en este documento académico. Para especificar los requisitos de la recopilación y el procesamiento de PHR centrados en el individuo (subpregunta 1), la sección "Requisitos para la recopilación y el procesamiento de PHR centrados en el paciente" proporciona el modelo de objetivos para el proceso interorganizativo descentralizado de e-salud centrado en la persona para la asistencia sanitaria pre-ventiva. Este modelo de objetivos sienta las bases para el diseño del sistema al recoger los principales requisitos funcionales y de calidad. Para determinar dónde surgen los conflictos (que se tratarán más adelante), la sección "Conflictos de privacidad entre los proveedores de asistencia sanitaria y los pacientes" (subcuestión 2) define los conflictos en el proceso descentralizado de sanidad electrónica y describe la correspondencia de los conflictos con objetivos funcionales y procesos empresariales específicos. Por último, para presentar las técnicas de resolución de conflictos, la sección "The Con-flict-Resolution Techniques When Mapping the BPMN-De-signed e-Healthcare Process to a Blockchain System" (sub-pregunta 3) propone técnicas en el sistema blockchain para resolver los conflictos identificados de definición automática de datos y reclamantes de forma transparente y descentralizada.

Requisitos para la recopilación y el procesamiento de datos PHR centrados en el paciente

Como afirman Norta y otros [53], un modelo de objetivos puede servir como herramienta analítica para examinar los problemas que surgen en un ámbito sociotécnico. Los modelos de objetivos actúan como interfaz para el intercambio de información entre las partes interesadas que poseen técnica y no técnica.

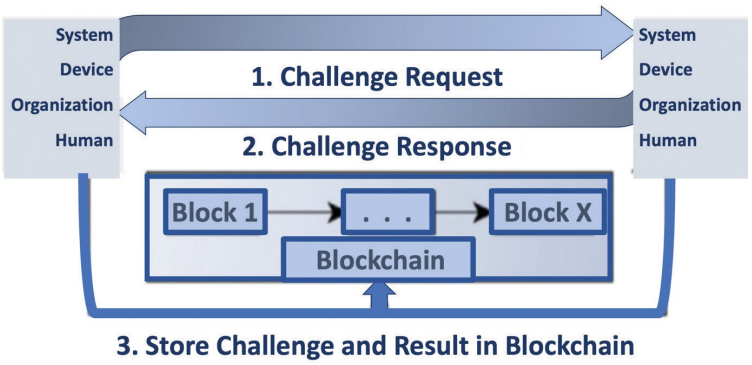

Fig. 3. Representación conceptual del ciclo de vida de (MFSSIA) Multi-factor challenge-set self-sovereign identity authentication para la gestión desafío-respuesta.

con el fin de generar un conocimiento comprensible del ámbito de la sanidad electrónica. Debido a la complejidad del modelo de objetivos, lo dividimos en dos partes: en la Figura 4 se definen los objetivos relacionados con el paciente y el profesional sanitario, y en la Figura 5 se incluyen los objetivos relacionados con el proveedor de seguros y el médico de cabecera. Las figuras 4 y 5 representan un modelo de objetivos en el que se definen objetivos funcionales, de calidad, emocionales positivos y negativos. Es importante señalar que cada objetivo funcional se subdivide a su vez en subobjetivos de forma jerárquica, situándose el nivel más alto en la parte superior y el más bajo en la parte inferior. En nuestra investigación anterior,[66] utilizamos el modelado de objetivos en la ingeniería de requisitos. Utilizamos la notación descrita en la Ref. 57, donde varios símbolos corresponden a diferentes tipos de objetivos. Así, la forma de corazón representa el objetivo emocional positivo, la forma de nube define los objetivos de calidad, y un paralelogramo representa los objetivos funcionales. En esta investigación, ampliamos la notación del modelo de objetivos con los objetivos funcionales toke-nizados que representan los objetivos funcionales que se comunican con una blockchain. En nuestro sistema diseñado, consideramos el contexto M2X, en el que los agentes pueden ser tanto humanos como no humanos.

Proponemos emplear un token de utilidad que se haya incorporado a un protocolo preexistente en la cadena de bloques y que se utilice para acceder a los distintos servicios ofrecidos por dicho protocolo. Estos tokens sirven como medio de pago por los servicios prestados dentro de sus respectivos ecosistemas en el sistema propuesto. Nuestra sugerencia es la introducción de un token denominado "Personal Health Token (PHT)" como token de utilidad para el sistema descentralizado de salud electrónica centrado en la persona.

Además del token de utilidad, proponemos el uso de tokens SBT creados por proveedores de datos médicos, como dispositivos inteligentes, sistemas PHR y EHR, que incluyan los datos médicos propiedad del paciente. Por ejemplo, si un paciente decide que algunos de sus datos sanitarios son útiles para la investigación médica, demuestra su propiedad con SBT a la empresa de investigación. El objetivo principal de la propuesta de valor es *prevenir enfermedades* en relación con un individuo que posee incentivos automotivados y prevé estar informado y capacitado durante todo el curso de acción preventiva. La principal propuesta de valor del sistema gira en torno a la prevención de enfermedades en los individuos. El subobjetivo de proporcionar asistencia domiciliaria implica que el paciente recoja sus datos médicos de forma fiable. El subobjetivo de proporcionar asistencia ambulatoria lo ejecuta el médico de cabecera, mientras que el subobjetivo de proporcionar un seguro lo lleva a cabo un proveedor de seguros. Además, el subobjetivo de dar de alta a los interesados lo realiza un agente aceptador. El objetivo de la parte interesada, que se encuentra dentro del sistema, es crucial para que las partes interesadas participen en el proceso inter-organizativo, mientras que llevan a cabo la verificación utilizando un protocolo conocido como MFSSIA, que se basa en la tecnología blockchain[64]La incorporación incluye el uso de tokens PHT para acceder a los servicios de autenticación. Tanto un profesional sanitario como un médico de cabecera presentan casos médicos al proveedor de seguros para solicitar reclamaciones. El objetivo inicial engloba dos subobjetivos adicionales: controlar el estado de salud ejecutado por el agente smart-hub y mantener un estilo de vida saludable dirigido por un especialista sanitario. Este último emplea el sistema, siempre que tenga seguridad en sí mismo, posea la capacidad de emitir juicios expertos y no se sienta abrumado por las complejidades del sistema.

El objetivo de monitorizar el estado de salud abarca tres subobjetivos: la generación de un PHR a partir de los datos recogidos por dos entidades, a saber, un smartwatch y un sensor doméstico de calidad del aire; el análisis semiautomatizado de dicho PHR; y la compartición segura del PHR, garantizando el procesamiento de información interoperable. La seguridad se consigue validando la SBT para garantizar la propiedad de los datos compartidos. El PHR producido posee la capacidad de integrarse sin fisuras, permitiendo su diseminación entre varias partes involucradas. Tras su creación, el PHR se inserta posteriormente en el libro mayor distribuido de la cadena de bloques, garantizando que pueda ser compartido.

Citación: Blockchain en la sanidad hoy 2023, **6**: 276 - https://doi.org/10.30953/bhty.v6.276

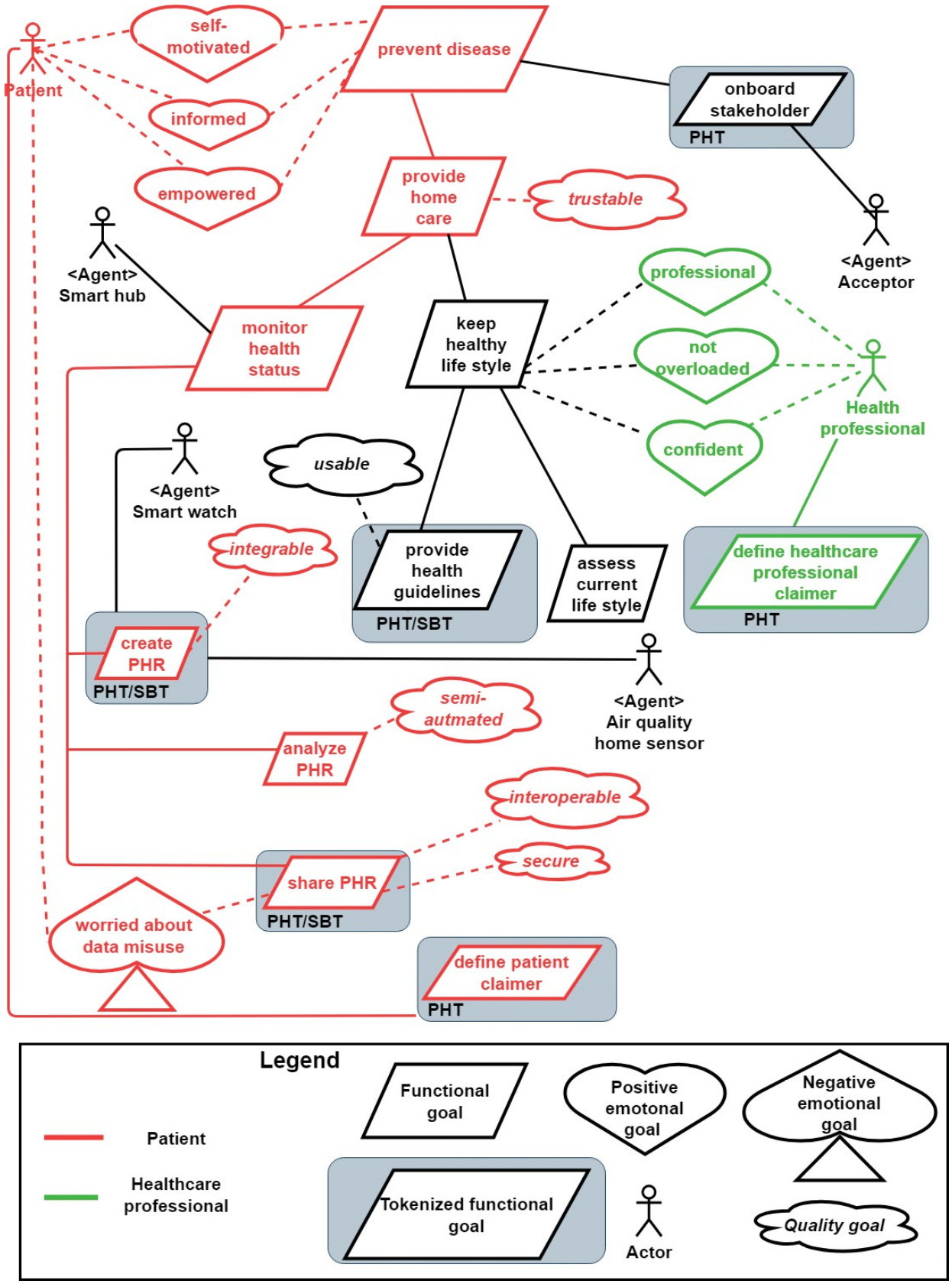

Fig. 4. Modelo de objetivos para un sistema descentralizado centrado en el individuo. Objetivos del paciente y del profesional sanitario.

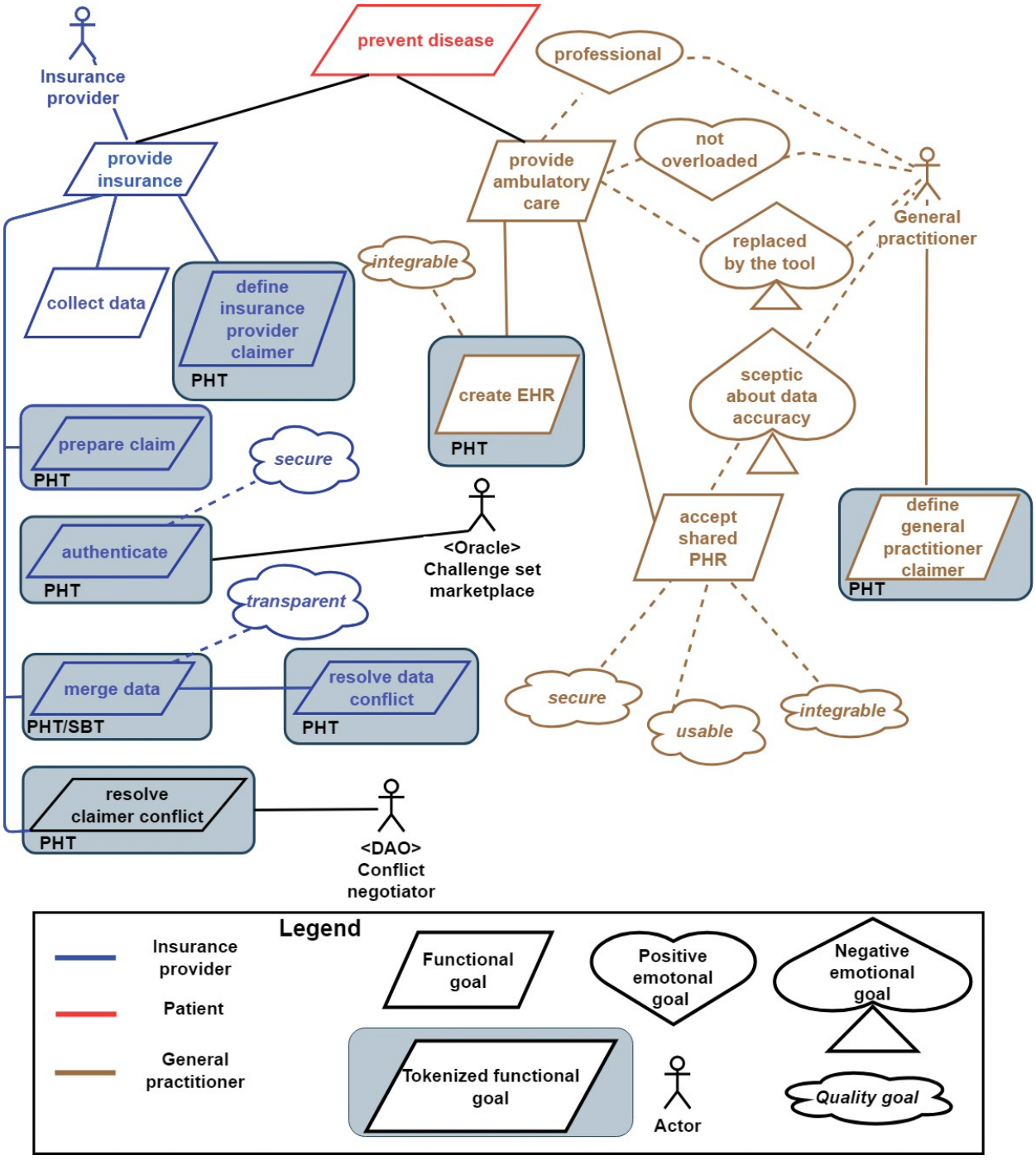

Fig. 5. Modelo de objetivos de un sistema descentralizado centrado en el individuo: objetivos del proveedor de seguros y del médico de cabecera.

El objetivo de lograr un estilo de vida saludable engloba dos subobjetivos específicos. El objetivo de lograr un estilo de vida saludable abarca dos subobjetivos específicos: evaluar el estilo de vida actual y ofrecer recomendaciones de salud. Las recomendaciones se comparten con el paciente a través de blockchain y deben ser utilizables.

El objetivo de proporcionar atención ambulatoria abarca la participación de un médico de atención primaria que alberga

Este objetivo se divide a su vez en tres subobjetivos: establecer un sistema de HCE interoperativo, adoptar un RPH compartido y administrar diagnósticos médicos. Este objetivo se divide a su vez en tres subobjetivos: establecer un sistema de HCE interoperable, adoptar un PHR compartido y administrar el diagnóstico médico. La HCE creada se almacena en una blockchain para que esté disponible para el paciente de forma segura e inmutable. Añadir datos

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

a la blockchain requiere PHT. Cuando un médico generalista se compromete a aceptar PHR, tiene reservas sobre la exactitud de los datos compartidos. Este fenómeno puede atribuirse al potencial de generación de datos erróneos o a la probabilidad de que un individuo alternativo reivindique la propiedad de los datos proporcionados. El proto-col MFSSIA apoya la forma autenticada y segura de producir datos médicos y elimina la desconfianza. Los datos médicos se almacenan con frecuencia en diversos estándares y contextos, lo que da lugar a una heterogeneidad semántica. El proceso de estandarización de los datos PHR y EHR ayuda a prevenir dicha heterogeneidad. Además, esta estandarización facilita la simplificación del procesamiento de los datos PHR y EHR. La aceptación segura, integrable y utilizable de los PHR es imperativa.

El objetivo del seguro proporcionado abarca un total de nueve subobjetivos, a saber: recopilación de datos, verificación, consolidación de datos, preparación de reclamaciones, resolución de conflictos entre reclamantes, definición de la reclamación del proveedor de seguros, definición de la reclamación del reclamante, definición de la reclamación del proveedor de asistencia sanitaria y definición de la reclamación del médico de cabecera. Los datos recopilados se utilizan durante el proceso de preparación de las solicitudes y requieren el proceso de autenticación de las distintas fuentes de datos dentro del marco interorganizativo, que se basa en el protocolo descentralizado conocido como MFSSIA. La autenticación se lleva a cabo mediante la utilización del mercado de conjuntos de retos, en el que el oráculo de la cadena de bloques facilita el suministro de conjuntos de retos seguros para la autenticación de usuarios. Para montar un siniestro, es imprescindible que el proveedor de seguros integre meticulosamente los datos de forma transparente, resolviendo los posibles conflictos que puedan surgir. Ambas acciones se realizan con contratos inteligentes. Dado que todas y cada una de las partes interesadas incorporan regula-ciones empresariales a sus respectivos objetivos funcionales (a saber, delimitar el reclamante para los proveedores de seguros, delimitar el reclamante para los pacientes, delimitar el reclamante para los proveedores de asistencia sanitaria y delimitar el reclamante para los médicos generalistas), resulta impera-tivo para el proveedor de seguros resolver cualquier conflicto que pueda surgir entre los reclamantes. Proponemos utilizar contratos inteligentes para que la resolución de conflictos sea transparente y, por tanto, fiable para las partes implicadas en los procesos interorganizativos. El negociador de conflictos, DAO, accede a los contratos inteligentes implementando la compleja lógica de los algoritmos de resolución de conflictos.

Conflictos de privacidad en el procesamiento integrado de PHR y EHR entre profesionales sanitarios y pacientes individuales

En el caso que nos ocupa, se supone que el proveedor de seguros está compuesto por tres socios: un paciente, un médico generalista afiliado a un hospital y un profesional sanitario, tal y como se muestra en la figura 1. Para cada

Se tienen en cuenta distintas reglas empresariales para cada parte interesada, que representan la identidad del reclamante y el receptor del pago del proveedor de seguros en circunstancias específicas. En nuestro escenario actual, se postula que el reclamante viene determinado por la medición de la presión arterial sistólica.

Según una norma empresarial, cuando la tensión arterial sistólica de un paciente desciende por debajo de 160 mmHg, se designa al paciente como demandante; en caso contrario, el demandante es un médico de cabecera. En la práctica habitual, una lectura de la presión arterial sistólica de 120 mmHg se considera un valor normal. Por lo tanto, el paciente no experimenta ningún problema en relación con la tensión arterial. La decisión se basa en el supuesto de que, en caso de que el paciente no experimente ninguna complicación, su modo de vida es loable y cumple los criterios para ser considerado beneficiario por el proveedor de seguros. Una tensión arterial sistólica que oscile entre 120 y 160 mmHg presenta problemas y requiere la atención y el compromiso diligentes del paciente para restablecerla en un rango normal. En consecuencia, el paciente también se percibe a sí mismo como demandante dentro de este intervalo de datos específico. Una tensión arterial sistólica superior a 160 mmHg plantea una situación peligrosa y requiere la atención de un médico. En consecuencia, el paciente ve al médico de cabecera como un demandante.

Según una normativa que regula las prácticas de un médico de atención primaria, se estipula que si la presión arterial sistólica de un paciente desciende por debajo de 120 mmHg, el paciente será clasificado como demandante; por el contrario, cuando la presión arterial sistólica supera la norma de 120 mmHg, el demandante asume el papel de médico general. En los casos en que la tensión arterial sistólica del paciente difiere de la norma prevista, el médico de atención primaria supervisa concienzudamente el estado del paciente y, posteriormente, administra los medicamentos y las intervenciones necesarias de acuerdo con las evaluaciones preliminares. En consecuencia, el médico de cabecera se percibe a sí mismo como un reclamante.

Para concluir, el profesional sanitario se adhiere a un conjunto de reglas de negocio que afirman lo siguiente: si la presión arterial sistólica del paciente es inferior a 120 mmHg, entonces el reclamante se clasifica como paciente; por el contrario, si la presión arterial sistólica supera los 160 mmHg, el profesional sanitario asume el papel de reclamante. En situaciones en las que la presión arterial sistólica se sitúa entre 120 y 160 mmHg, los profesionales sanitarios ejercen su discreción a la hora de identificar explícitamente al reclamante.

La aparición de conflictos puede atribuirse a los reglamentos internos de las tres entidades implicadas, como se ilustra en la figura 6. Estos conflictos se hacen patentes cuando la presión arterial sistólica de un paciente supera el umbral predeterminado de 120 mmHg.

Funciones en las que se producen conflictos

En esta sección, definimos los objetivos funcionales presentados en el modelo de objetivos de las figuras 4 y 5 en los que se producen conflictos. Para simplificar la investigación, hemos optado por excluir los conflictos que puedan surgir en relación con los objetivos de calidad y emocionales. La correlación entre los objetivos funcionales y los posibles conflictos se ha pre-sentado en la Tabla 1.

En nuestro caso, se consideran dos posibles conflictos durante el proceso interorganizativo de reclamación de seguros. En primer lugar, puede surgir un conflicto de datos cuando un proveedor de seguros recopila y consolida datos de varias fuentes, como el sistema PHR del paciente, el sistema EHR del proveedor sanitario y los registros del profesional sanitario. Dado que cada parte interesada puede mantener los datos en formatos y estándares distintos, existe la posibilidad de que los datos fusionados no se correspondan o sincronicen adecuadamente cuando el proveedor de seguros los integre, dando lugar a datos incongruentes o contradictorios.

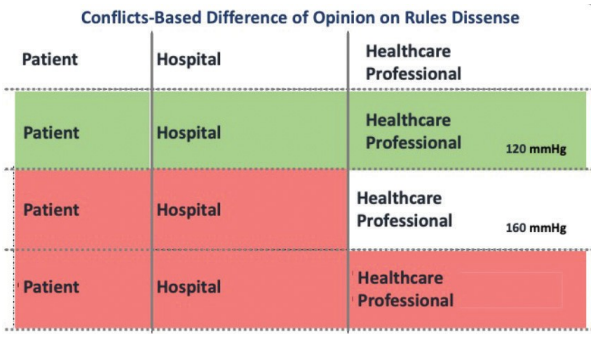

Fig. 6. Se ha observado que la aplicación de las normas empresariales da lugar a conflictos de comportamiento.

En segundo lugar, puede surgir un conflicto de definición del reclamante cuando cada parte interesada define al reclamante del seguro basándose en sus normas empresariales internas y en el valor de los datos, como la lectura de la tensión arterial del paciente. Como se ilustra en la Figura 6, las reglas para proponer una reclamación por parte del paciente, el proveedor de atención sanitaria y el profesional sanitario pueden diferir en función de las circunstancias de los datos. Por ejemplo, si la tensión arterial del paciente se sitúa entre 120 y 160 mmHg, el paciente y el profesional sanitario propondrán reclamaciones diferentes en función de sus distintas reglas. La incongruencia entre la definición del demandante da lugar a un conflicto que requiere resolución.

Procesos en los que se producen conflictos

La definición de un reclamante de seguros implica la recuperación de datos de fuentes de datos PHR y EHR, seguida de su integración y la eliminación de datos irrelevantes. El proceso de definición de un reclamante proveedor de seguros se define en la figura 7. Para facilitar el proceso de definición interorganizacional del reclamante, lo hemos subdividido en

Tabla 1. Objetivos funcionales en los que se producen conflictos. Objetivos funcionales en los que se producen conflictos.

Objetivo funcional	Actor	Conflicto
Recoger datos	Proveedor de seguros	Los datos pueden ser diferentes
Fusionar datos	Proveedor de seguros	Los datos pueden ser diferentes
Definir el proveedor de seguros reclamante	Proveedor de seguros	El reclamante puede ser diferente
Definir paciente reclamante	Paciente	El reclamante puede ser diferente
Definir reclamante profesional sanitario	Profesional sanitario	El reclamante puede ser diferente
Definir médico generalista reclamante	Médico generalista	El reclamante puede ser diferente

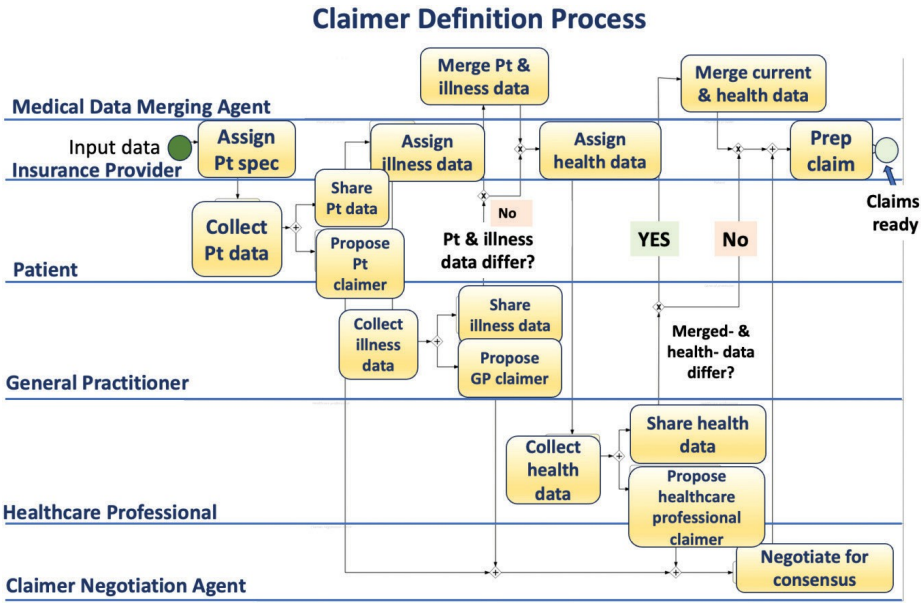

Fig. 7. Proceso de definición del reclamante para el proveedor de seguros.

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

tres subprocesos, a saber, el proceso de toma de decisiones para los profesionales sanitarios, los proveedores sanitarios y los pacientes. Además, expondremos estos tres procesos internos utilizando la notación BPMN.

La figura 8 ilustra el proceso interno de toma de decisiones emprendido por el paciente, dirigido por las reglas de negocio descritas anteriormente. Al principio, el paciente comprueba la presencia de los datos solicitados a la compañía de seguros en su repositorio PHR. En caso de que los datos solicitados no estén presentes, el paciente procede a registrar las mediciones de la presión arterial y posteriormente almacena estos nuevos datos en el repositorio PHR. Posteriormente, el paciente recupera dichos datos del repositorio PHR y los comparte con otras partes interesadas en el proceso interorganizativo. Por último, para proponer al reclamante, se evalúa el valor de la presión arterial. Si el valor de la presión arterial es igual o inferior a 160 mmHg, el paciente se autoproclama reclamante.

Por el contrario, si el valor de la tensión arterial es superior a 160 mmHg, se propone al profesional sanitario como reclamante.

La figura 9 ilustra el proceso interno de toma de decisiones de un proveedor de asistencia sanitaria, por ejemplo un hospital. Inicialmente, el proveedor sanitario adquiere los datos de la enfermedad (HCE) de sistemas HCE externos, que pueden estar afiliados a un hospital. Una vez obtenidos los datos de HCE externos, se transforman en el estándar de datos sanitarios del proveedor de asistencia sanitaria y se almacenan en su propio sistema. Posteriormente, los datos externos importados se difunden entre los demás participantes en el proceso interorganizativo. Por último, la propuesta de reclamante del proveedor de asistencia sanitaria se formula sobre la base de las reglas de negocio descritas en la sección "Conflictos de privacidad en el procesamiento integrado de PHR y EHR entre proveedores de asistencia sanitaria y pacientes individuales". Esta proposición abarca tres demandantes potenciales: el paciente, el proveedor sanitario y un demandante no definido. En concreto, si el valor de la tensión arterial es

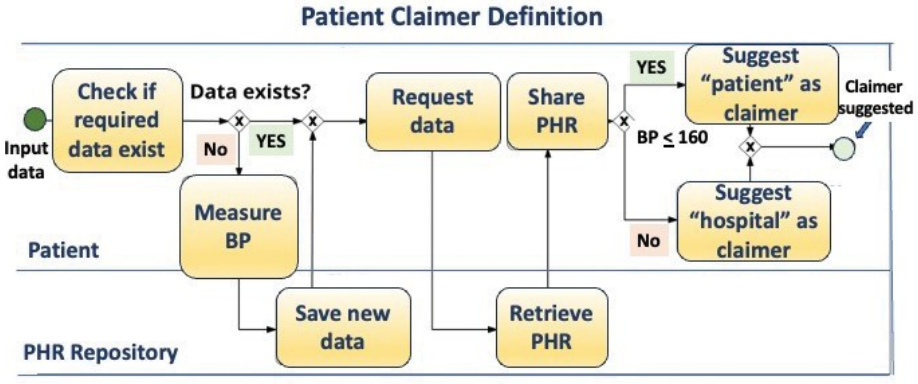

Fig. 8. Proceso de decisión interno de la reclamación del paciente. PA: presión arterial; DAO: Organizaciones Autónomas Descentralizadas; PHR: historia clínica personal.

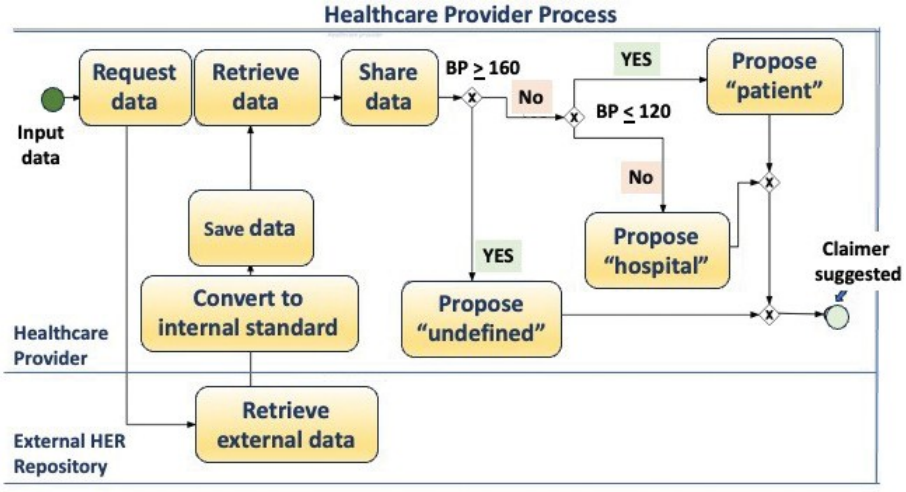

Fig. 9. Proceso interno de toma de decisiones de los proveedores sanitarios con respecto a los reclamantes. PA: presión arterial (presión arterial sistólica en este caso).

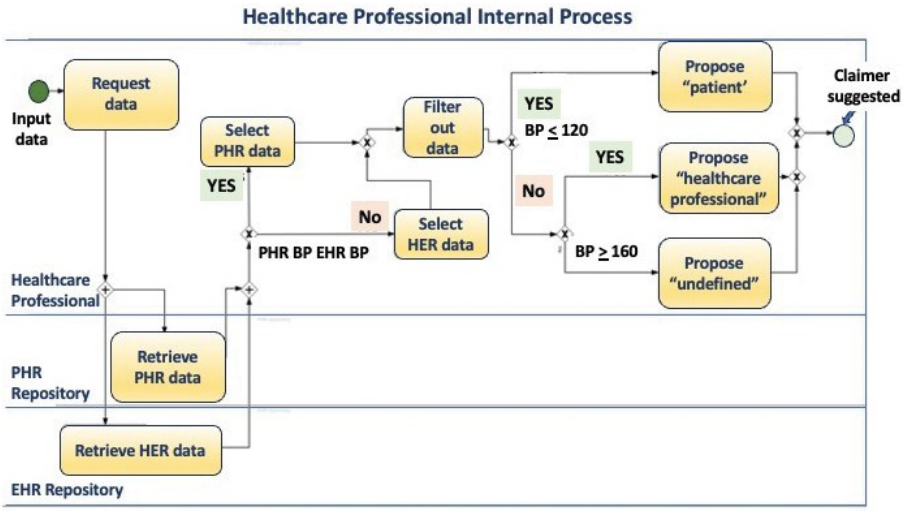

Fig. 10. Los profesionales sanitarios afirman que el proceso interno de toma de decisiones desempeña un papel crucial en su práctica. PA: tensión arterial (tensión arterial sistólica en este caso); HCE: historia clínica electrónica; HCP: historia clínica personal.

igual o inferior a 120 mm Hg, se sugiere al paciente como demandante. En última instancia, se sugiere al profesional sanitario como asertor en caso de que la tensión arterial se sitúe en el intervalo de 120 y 160 mm Hg.

La figura 10 describe el proceso interno de toma de decisiones en el ámbito de los profesionales sanitarios. En particular, la disparidad entre los procesos de toma de decisiones de pacientes y profesionales sanitarios radica en la capacidad de los profesionales sanitarios para acceder tanto a los datos de la HCE como a los de la HSP. En un primer momento, las mediciones de la presión arterial se obtienen simultáneamente de las bases de datos PHR y EHR. Posteriormente, tras eliminar los datos extraños, el profesional sanitario propone un demandante. En caso de que la presión arterial sea igual o inferior a 120 mmHg, se presenta una reclamación al paciente. Sin embargo, si la presión arterial se sitúa entre 120 y 160 mmHg, el demandante permanece indefinido. Por último, si la tensión arterial supera o es igual a 160 mmHg, el profesional sanitario se presenta como reclamante. La incorporación de la integración de HCE y RPH se basa en nuestra investigación anterior[66], mientras que las normas para la propuesta de reclamante se exponen en la Figura 6.

Técnicas de resolución de conflictos al trasladar el proceso de atención sanitaria electrónica diseñado por Bpmn a un sistema Blockchain

En esta sección, presentamos las técnicas de resolución de conflictos que apoyan la resolución automática de los conflictos que se producen en los procesos interorganizativos de la sanidad electrónica. En nuestro caso, dos posibles conflictos se derivan de las diferencias entre las normas empresariales internas o los datos médicos recopilados.

Este estudio plantea la utilización de una DAO como mecanismo de resolución de con-flictos en sistemas de e-salud descentralizados. El proceso de resolución de conflictos en el proceso del proveedor de seguros se representa en la figura 11. Inicialmente, el proveedor de seguros recopila datos médicos de tres fuentes, a saber, pacientes, proveedores sanitarios y médicos de cabecera, para preparar una reclamación. Posteriormente, los datos recopilados se someten a validación para comprobar su integridad. Tras el proceso de validación, la DAO aprueba o desaprueba la validez de los datos. En función del resultado final de la validación, puede generarse una solicitud.

En la figura 12 se explica con más detalle cómo se realiza la validación de datos de una única fuente de datos. El proceso exacto se realiza para los tres propietarios de los datos médicos: paciente, proveedor sanitario y médico de cabecera. La DAO emplea un algoritmo de consenso que requiere que todos los nodos reevalúen los datos entrantes. Los datos sólo se consideran válidos si una mayoría de nodos, superior al 50%, coincide en que son exactos. Por el contrario, si los datos no obtienen un acuerdo suficiente, se consideran manipulados y, por consiguiente, no aptos para su utilización en la preparación de reclamaciones.

Por último, el proceso de validación de datos médicos de un único nodo se describe en la figura 13 en el contexto de la validación global de datos gestionada por la DAO. En este proceso, cada nodo de la cadena de bloques afiliado a la DAO realiza un examen de los datos médicos sometidos a escrutinio. El nodo solicita datos médicos específicos, como la lectura de la tensión arterial, a la fuente de datos original, como el sistema PHR del paciente. A continuación, el nodo compara los datos de la fuente con los datos validados en la cadena de bloques. Si los datos coinciden exactamente, el nodo los considera válidos y lo confirma mediante su voto en el algoritmo de consenso. En caso de que los datos no coincidan, se produce una disparidad entre la fuente de datos inicial y los datos almacenados en la blockchain. En este caso

Citación: Blockchain en la sanidad hoy 2023, **6**: 276 - https://doi.org/10.30953/bhty.v6.276

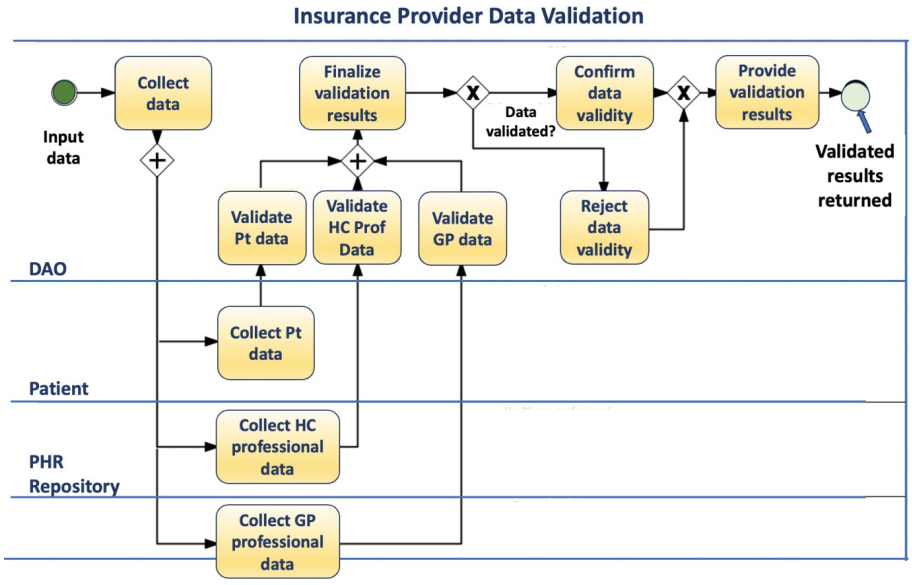

Fig. 11. Proceso de resolución de conflictos de datos de proveedores de seguros. DAO: Organizaciones Autónomas Descentralizadas; Pt: paciente; GP: médico generalista; HC: asistencia sanitaria.

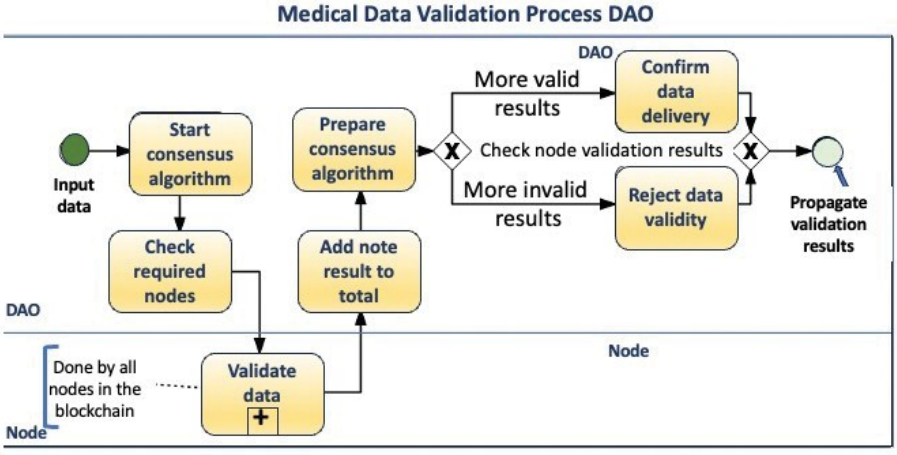

Fig. 12. Proceso de validación de datos de las DAO. DAO: Organizaciones Autónomas Descentralizadas.

circunstancias, el nodo considera que los datos no son válidos o han sido manipulados, por lo que los descarta mediante un proceso de votación que se opone a su validez dentro del algoritmo consen-sus.

Hacer que cada nodo compruebe directamente los datos desde la fuente puede identificar problemas de manipulación de datos, incluso si un subconjunto de nodos son maliciosos. El algoritmo de consenso verifica los datos válidos si la mayoría de las comprobaciones de validación de los nodos tienen éxito. Esta validación redundante por parte de cada nodo proporciona una mayor seguridad y precisión en la identificación de la manipulación de datos que confiar en un validador centralizado.

En la arquitectura descentralizada que hemos propuesto, las unidades individuales conocidas como "nodos" participan en un proceso de toma de decisiones para validar la exactitud e integridad de los datos. Este proceso se rige por una DAO, que sirve para resolver conflictos. Cada nodo emite un voto para confirmar o rechazar la validez de los datos en cuestión. Una vez recogidos todos los votos, se toma una decisión final basada en el con-senso mayoritario entre los nodos. En esencia, si la mayoría de los nodos llega a un consenso sobre la validez de los datos, éstos se consideran aceptables; en caso contrario, se consideran inaceptables y, por tanto, se rechazan. Este enfoque demo-crático garantiza un proceso de validación más sólido y transparente.

Evaluación y debate

En esta sección se presenta la evaluación de este trabajo utilizando el enfoque de evaluación multimétodo que infiere DSR. En primer lugar, realizamos una evaluación formal con CPN y, a continuación

proporcionamos la discusión de los resultados de la evaluación de la CPN y las implicaciones de los principales resultados de este trabajo con otra literatura relacionada. A continuación, presentamos un prototipo PoC que implementa el flujo de trabajo evaluado por la CPN.

En primer lugar, evaluamos el proceso de resolución de conflictos con el modelado de la CPN. El proceso de resolución de conflictos en el modelo CPN tiene varias capas. La capa superior son los procesos internos de las partes interesadas. A continuación, se presenta la evaluación de la CPN dada, seguida de la implementación del prototipo PoC. Por último, se discuten los resultados actuales comparados con investigaciones similares.

Evaluación formal de la CPN del proceso de resolución de conflictos de definición de reclamante

La red de Petri clásica es un grafo bipartito dirigido con dos tipos de nodos denominados lugares y transiciones. Los nodos se conectan mediante arcos dirigidos. No se permiten conexiones entre dos nodos del mismo tipo. Los lugares se representan mediante círculos y las transiciones mediante rectángulos[67].

Para evaluar la caracterización del demandante del proceso de resolución de conflictos, proponemos un modelo CPN estructurado[68]para la identificación y rectificación de posibles deficiencias de diseño, ausencia de especificaciones, así como problemas de seguridad y privacidad.

La descripción completa del modelo CPN figura en el informe técnico[68].Nuestro modelo de evaluación se centra en un proceso descentralizado de intercambio de datos y omite todos los objetivos funcionales definidos en las figuras 4 y 5. Estos objetivos están relacionados con la aparición y resolución de conflictos.

Estos objetivos están relacionados con la aparición y resolución de conflictos. Los objetivos cubiertos por el modelo CPN son:

- Proponer un reclamante de seguros
- Recopilar datos
- Compartir PHR
- Resolver el conflicto de datos
- Resolver el conflicto del reclamante.

Utilizamos la formalización del marco eSourcing,[69]donde se incluyen las redes de flujo de trabajo (WF-nets). Así, los modelos CPN para los procesos internos de las partes interesadas son arranged, por lo que el flujo de control se asemeja a la for-malización eSourcing. WF-net define el comportamiento dinámico de un solo caso aislado.

Las WF-nets son una formalización para describir modelos de proceso en sistemas paralelos y distribuidos[70]Research[71]describe una WF-net como una red de Petri que tiene una 3-tupla $N = (P,T,F)$, donde P y T son dos conjuntos disjuntos y finitos que son, respectivamente, llamados lugares (los círculos los visualizan) y transiciones (los rectangles l o s representan), y $F \subseteq (P \times T) \cup (T \times P)$ es un conjunto de relaciones de flujo en N. El conjunto F es un subconjunto de la unión del producto cartesiano de P y T con el producto cartesiano de T y P. $P \times T$ representa el producto cartesiano de los conjuntos P y T. El producto cartesiano consiste en todos los pares ordenados posibles donde el primer elemento es del conjunto P, y el segundo elemento es del conjunto T.

La figura 14 muestra la WF-net que tiene un único lugar de inicio y un único lugar final con un token en el lugar de inicio (todos los demás lugares están vacíos). Todos los nodos conducen del lugar inicial al final, de modo que cuando se completa la promulgación, sólo hay un token en el lugar final único, y todos los demás lugares están vacíos[11]Debe tenerse en cuenta que una WF-net especifica el comportamiento dinámico de un caso único.

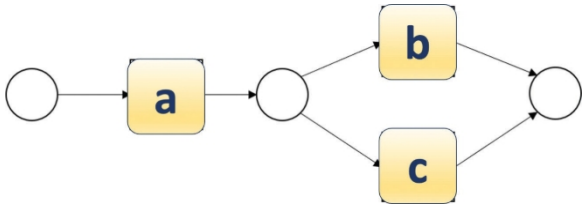

Fig. 14. Ejemplo de red de flujo de trabajo. Ejemplo de red de flujo de trabajo[72].

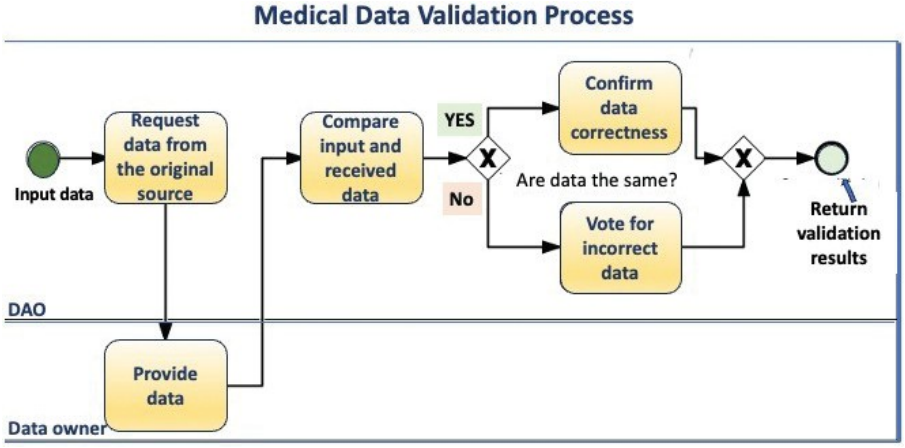

Fig. 13. Proceso de validación de datos de nodo. DAO: Organizaciones Autónomas Descentralizadas.

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

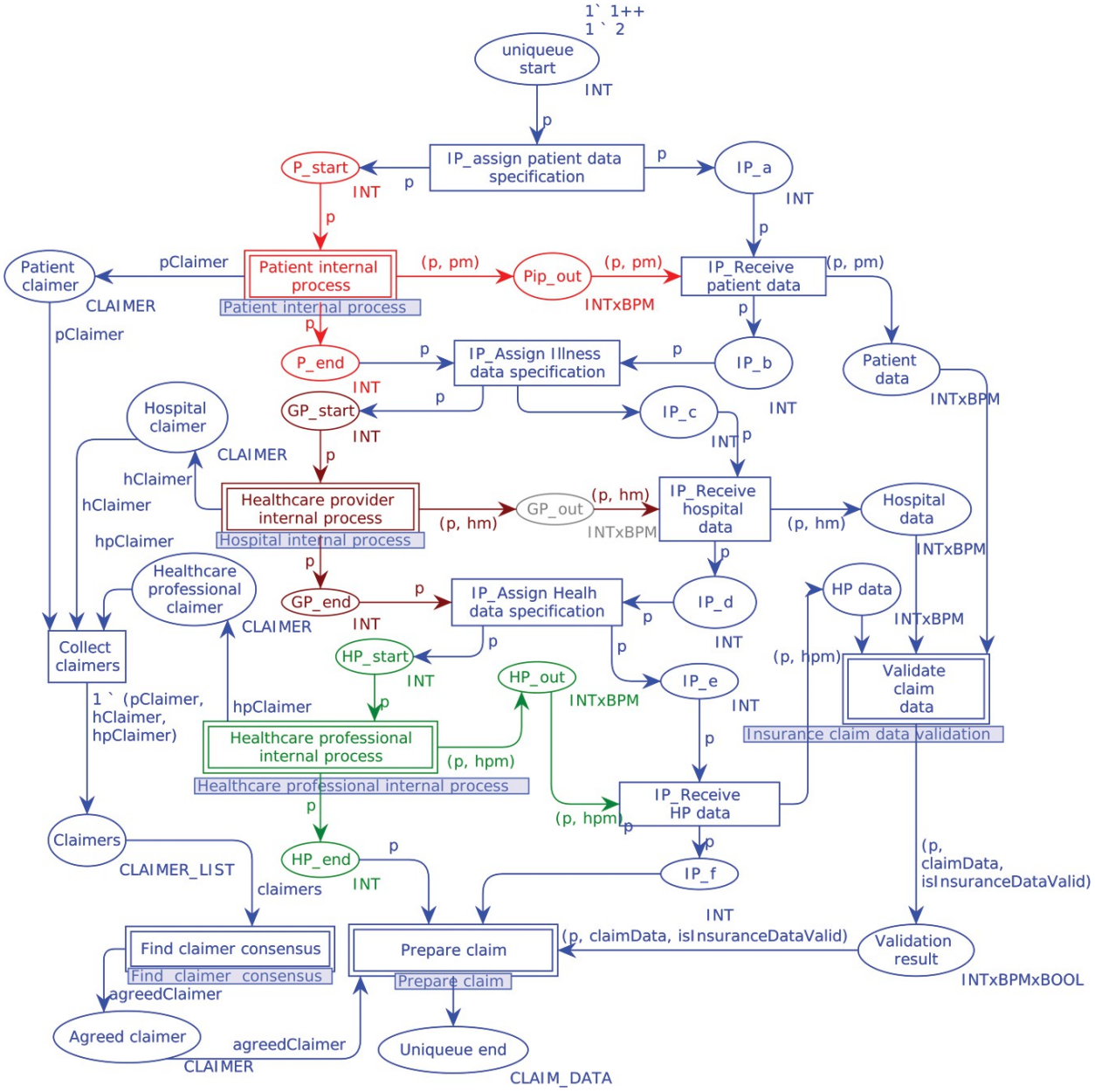

Fig. 15. La capa externa del modelo CPN define el proceso interorganizativo. CPN: Redes de Petri coloreadas.

de forma aislada. Esto significa que cada pieza de trabajo se ejecuta para un caso específico, que también se denomina instancia de flujo de trabajo[67]

Configuración formalizada de nivel superior

La figura 15 ilustra los aspectos procedimentales implicados en la formulación de una reclamación que abarca múltiples entidades organizativas. Para montar una reclamación médica, el proveedor de seguros obtiene datos sanitarios de diversos orígenes, como historiales de pacientes, sistemas de proveedores sanitarios y sistemas utilizados por especialistas sanitarios. Los procesos internos de recopilación de datos y definición de reclamaciones implican la interacción con los sistemas descentralizados de las partes interesadas. descentralizados. Utilizamos diferentes colores para los procesos internos con el fin de visualizar mejor un proceso interorganizativo. El proceso interno del paciente se muestra en rojo, el del profesional sanitario en marrón y el del profesional sanitario en verde.

Nuestro modelo CPN se basa en los procesos BPMN definidos anteriormente en este artículo. Todo el proceso de definición del reclamante pro-vidente de seguros se deriva de la Figura 10. Las capas CPN que definen los procesos que encapsulan la definición interna del reclamante de la lógica empresarial se basan en los procesos BPMN. El modelado de los procesos internos de definición del reclamante permite la aparición de conflictos y la simulación al evaluar el modelo CPN. El mapeo entre los diagramas BPMN y las capas del modelo CPN de reclamaciones de pacientes,

paciente, profesional sanitario y proveedor sanitario se muestra en la Tabla 2.

El proceso de preparación de reclamaciones parte de un único lugar de inicio con dos tokens que describen identificadores de proceso independientes. El diseño del modelo admite varias ejecuciones paralelas del proceso al proporcionar identificadores de proceso para cada lugar. Todas las transiciones realizadas por el proveedor de seguros están marcadas con color azul y comienzan con el prefijo IP_. Posteriormente, se instiga el inicio de la transición IP_asignar especificación de datos del paciente, comenzando así el proceso interno del paciente. El proceso interno del paciente tiene dos salidas: la medición de la tensión arterial y la propuesta del reclamante. El mismo flujo de trabajo existe tanto para los proveedores como para los profesionales sanitarios. La definición del reclamante se basa en las reglas internas descritas en la figura 6.

Cuando se ejecutan los tres procesos internos, se activa la transición Recopilar reclamantes con tres entradas que definen el reclamante propuesto por cada parte interesada. La transición Encontrar reclamante consensuado procesa los tres reclamantes propuestos y selecciona uno basándose en el algoritmo de consenso.

Antes de que se pueda preparar una reclamación, otro proceso se ejecuta en paralelo con la definición del reclamante: la validación de la medición de la presión arterial recogida. Este proceso verifica el posible compromiso de los datos y, posteriormente, resuelve las discrepancias que puedan surgir en caso de divergencia de datos. Una vez que los algoritmos de consenso concuerdan con las mediciones del reclamante y de la presión sanguínea, tiene lugar la transición de la reclamación Prepare.

Flujos de trabajo internos de las partes interesadas interorganizativas que procesan HCE y RPH integradas

Para representar los flujos de trabajo de las distintas partes interesadas, empleamos transiciones de sustitución que implican subredes que detallan las actividades vinculadas a una transición. La subred vinculada a una transición suele denominarse subpágina en el discurso académico. La utilización del formalismo CPN permite la organización jerárquica de subpáginas hasta un grado indefinido, facilitando así la representación de descripciones de sistemas a diversos niveles de complejidad[73]

Para mejorar el escenario de colaboración, lo ampliamos con una simulación que utiliza CPN. Además, incorporamos el escenario de conflicto al modelo cuantitativamente simulable. Para organizar el modelo CPN general,[2] lo dividimos en múltiples subpáginas, como se muestra en la Tabla 3.

La figura 16 muestra una captura de pantalla derivada de las herramientas CPN, que presenta la disposición jerárquica de las subpáginas dentro del modelo de diseño. Estas subpáginas, que sirven

[2]https://goo.by/JOQJ8

Tabla 2. Mapeo del proceso de definición del reclamador interno desde diagramas BPMN
a las capas del modelo CPN.

Proceso BPMN	Capa CPN
Proceso interno de decisión del reclamante paciente (Figura 8)	Proceso interno del paciente
Proceso de decisión interno reclamante-proveedor sanitario (Figura 9)	Proceso interno del proveedor de asistencia sanitaria
Proceso de decisión interno del reclamante profesional sanitario (figura 10)	Proceso interno del profesional sanitario

BPMN: Modelo y Notación de Procesos de Negocio; CPN: Redes de Petri coloreadas.

como componentes reutilizables, contribuyen a mejorar la comprensibilidad del intrincado modelo. Dentro de este marco, la página principal, denominada "Externa", asume el papel de delinear el protocolo interorganizacional para la preparación de una reclamación al seguro. Los procedimientos internos de las distintas partes interesadas, a saber, el proceso interno del paciente, el proceso interno del hospital y el proceso interno del profesional sanitario, se engloban en subpáginas separadas. La resolución de conflictos se lleva a cabo en un nivel superior del proceso, concretamente dentro de las subpáginas dedicadas a la validación de los datos de la reclamación de seguro y a la consecución de un consenso entre los reclamantes.

Evaluación del modelo CPN

Evaluamos nuestro modelo utilizando dos enfoques diferentes. En primer lugar, evaluamos el modelo original mediante simulación en CPN Tools, asegurándonos de que todas las fichas iniciales conducen al único estado final del modelo. Dada la complejidad del modelo CPN proporcionado, realizamos un análisis del espacio de estados para cada subpágina individualmente. Si la página incorpora alguna de las subpáginas, imitamos su salida. Esta imitación consiste en sustituir la ejecución real de la subpágina por un único elemento que genere datos constantes. De este modo, mantenemos la integridad del flujo de la página principal y reducimos la complejidad del análisis del espacio de estados. Los valores predeterminados se establecen en función de los posibles resultados de la subpágina. A lo largo del análisis del espacio de estados, calculamos y presentamos todos los estados alcanzables y los cambios de estado del modelo CPN como un grafo dirigido. El gráfico presenta los estados como nodos y los sucesos como arcos. El objetivo principal del análisis del espacio de estados es describir el comportamiento del sistema y comprobar que no hay bloqueos, que siempre se puede alcanzar un estado determinado y que siempre se presta un servicio determinado[71].

El informe sobre el espacio de estados da cuenta de las propiedades de origen y de vitalidad. Las primeras se refieren a una marca de inicio específica que es accesible desde cualquier marca alcanzable. En nuestro escenario, cada proceso asociado a una subpágina alcanzará finalmente su estado ter-minal. Por otro lado, las propiedades de liveness delimitan las marcas sin elementos vinculantes activos. Un marcado sin actividad puede ser tanto un marcado muerto

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

Tabla 3. Subpáginas en el modelo CPN Subpáginas en la jerarquía del modelo CPN.

Subpágina	Significado
Proceso interno del paciente	Procesos de recogida de datos del paciente y definición del reclamante
Proceso interno del hospital	Procesos de recogida de datos y definición de reclamaciones de médicos de cabecera
Proceso interno del profesional sanitario	Procesos de recogida de datos de profesionales sanitarios y definición de reclamantes
Manipulación de datos	Proceso de manipulación de datos que tiene lugar durante la recogida de datos
Recogida de datos	Proceso de recogida de datos
Definición del paciente demandante	Proceso de definición del reclamante paciente
Definir reclamante profesional sanitario	Proceso de definición del reclamante profesional sanitario
Definición de reclamante hospitalario	Proceso de definición del reclamante hospitalario
Validación de datos de reclamaciones de seguros	Proceso de validación de todos los datos recopilados de las distintas partes interesadas
Validación de datos	Proceso de validación de la medición de la presión arterial por varios nodos
Validación de nodos	Proceso de validación de la medición de la presión arterial realizado por un único nodo
Buscar el consenso de los declarantes	Proceso de consenso sobre el reclamante final

CPN: Redes de Petri coloreadas.

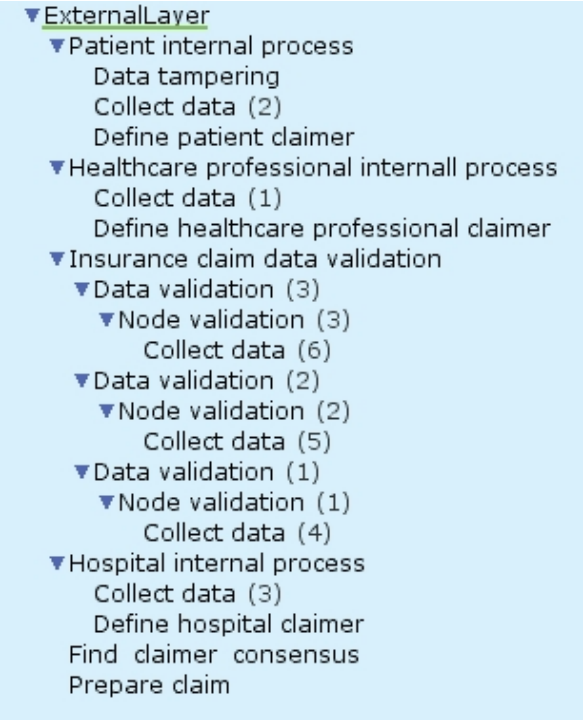

Fig. 16. Jerarquía de páginas del modelo CPN. CPN: Redes de Petri coloreadas.

y una marca de inicio simultáneamente, ya que se puede acceder a cualquier marca desde sí misma a través de una secuencia de ocurrencia trivial de longitud cero. A continuación, el informe del espacio de estados delinea las transiciones en vivo. En un contexto académico, una transición se considera viva cuando es perpetuamente factible identificar una secuencia de ocurrencias que incluya la transición desde cualquier marca alcanzable. El informe del espacio de estados proporciona una relación de las transiciones inactivas. Una transición se clasifica como inactiva si está habilitada o es inalcanzable. Estas transiciones delinear la funcionalidad de un modelo que nunca puede ejecutarse.[74]

Todos los informes que analizan el espacio de estados se basan en cada subpágina que se encuentra dentro del modelo CPN presentado, como se indica en las tablas correspondientes que se proporcionan más adelante. Los archivos ini-ciales del informe de análisis del espacio de estado pueden consultarse en línea.[3]

Según los resultados presentados en la Tabla 4, es evidente que los bucles son inherentes al proceso de recopilación de datos. El repositorio de datos contiene información sobre varios procesos, y el proceso de recopilación de datos continúa recuperando datos hasta que localiza información asociada al proceso en curso. Todas las subpáginas de nuestro proceso no contienen transiciones muertas y vivas, lo que indica la ausencia de componentes no utilizados. En particular, el estado de todas las subpáginas coincide con el de las marcas de inicio y muerto.

Proof-of-Concept Prototype Implementation for the Running Case Este estudio presenta la implementación de un prototipo para el proceso de compartición de datos de e-salud[75]desarrollado en el ámbito de la Ref. 76. En nuestro contexto específico, proponemos la utilización de Polygon[77]Smart Contracts (SCs) para el sistema de proveedores de seguros. Al mismo tiempo, se recomiendan los SC de Ethereum para los sistemas de pacientes, hospitales y profesionales sanitarios. La red Polygon se basa en una arquitectura de cadena de bloques de alto rendimiento, en la que cada punto de control selecciona un grupo de productores de bloques para lograr el consenso. La validación de los bloques se realiza a través de una capa PoS, que también actualiza periódicamente la red principal de Ethereum con las pruebas proporcionadas por los productores de bloques. Para mejorar la escalabilidad y permitir la interoperabilidad entre diferentes sistemas basados en cadenas de bloques, empleamos Polkadot[78], que facilita la comunicación segura y libre de confianza entre cadenas de bloques especializadas.

[3]https://goo.by/QaISC

Tabla 4. Resultados del análisis del espacio de estados para las subpáginas del modelo CPN.

Subpágina	Bucles	Marcado de inicio	Marcado muerto	Transiciones muertas	Transiciones en vivo
Proceso interno del paciente	No	Sí	Sí	No	No
Proceso interno de los profesionales sanitarios	No	Sí	Sí	No	No
Proceso interno del hospital	No	Sí	Sí	No	No
Definir paciente reclamante	No	Sí	Sí	No	No
Definir reclamante profesional sanitario	No	Sí	Sí	No	No
Definir reclamante hospitalario	No	Sí	Sí	No	No
Buscar consenso de reclamantes	No	Sí	Sí	No	No
Recoger datos	Sí	Sí	Sí	No	No
Manipulación de datos	No	No	Sí	No	No
Validación de datos	No	Sí	Sí	No	No
Validación de nodos	No	Sí	Sí	No	No
Capa externa	No	Sí	Sí	No	No
Preparar la solicitud	No	Sí	Sí	No	No

CPN: Redes de Petri coloreadas.

En el entorno web descentralizado facilitado por la capa fundacional de Polkadot, los usuarios ejercen autoridad sobre sus datos. Este prototipo consta de tres elementos principales basados en blockchain. En concreto, engloba dos aplicaciones distintas para la introducción de historiales médicos, a saber, los del paciente y los del médico. Además, incorpora una aplicación que ejecuta el procedimiento interorganizacional que implica al proveedor de seguros junto con un contrato inteligente DAO que lleva a cabo la comparación de datos en caso de conflictos y proporciona datos fiables. El prototipo PoC que nos ocupa se centra en el escenario en el que el paciente y el médico introducen las mediciones de la presión sanguínea.

La figura 17 presenta una captura de pantalla de la interfaz de la aplicación del paciente, que muestra explícitamente la introducción de las mediciones de la presión arterial. Esta aplicación está integrada con el monedero Metamask, lo que permite compartir los datos introducidos a través de un contrato inteligente. En particular, la aplicación incorpora el despliegue de un contrato inteligente en la Blockchain de Ethereum.

La figura 18 representa visualmente un conflicto que surge durante la recogida de datos. El escenario representado ejemplifica una discrepancia entre las mediciones de la presión arterial registradas por el paciente y las documentadas por el médico. En estos casos, los datos se transmiten a una DAO, que asume la responsabilidad de validarlos y resolver los posibles conflictos.

El proceso interorganizativo se implementa con la cadena de bloques Polkadot, que permite la comunicación entre cadenas de bloques. Implementamos un módulo basado en blockchain específico de la aplicación con el marco Substrate[79]. La aplicación del proveedor de seguros se ejecuta como un nodo local backend de Substrate.

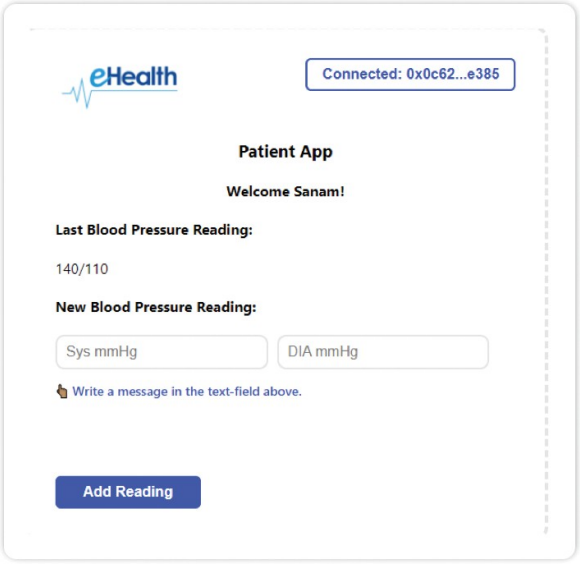

Fig. 17. Captura de pantalla de la aplicación de un paciente.

Debates sobre las implicaciones de la investigación en trabajos similares

Esta investigación propone que blockchain permita la resolución autónoma de conflictos de forma transparente y sin un único punto de confianza. Además, las tecnologías de cadenas de bloques y contratos inteligentes permiten ofrecer servicios personalizados de sanidad electrónica que incluyen a varias partes interesadas, al tiempo que garantizan la propiedad individual de los datos sanitarios. El auge de la economía M2X y de los agentes no humanos en los procesos interorganizativos requiere nuevos métodos de autenticación basados en el mecanismo de conjunto de desafíos multifactoriales. Este enfoque permite nuevos procesos interorganizativos en situaciones de falta de confianza entre las partes interesadas. La evaluación con CPN muestra que un proceso de este tipo puede ser viable con el ejemplo del seguro de salud electrónico descentralizado. Sin embargo, no disponemos de pruebas empíricas in vivo de que esto sea así.

Citación: Blockchain en la sanidad hoy 2023, 6: 276 - https://doi.org/10.30953/bhty.v6.276

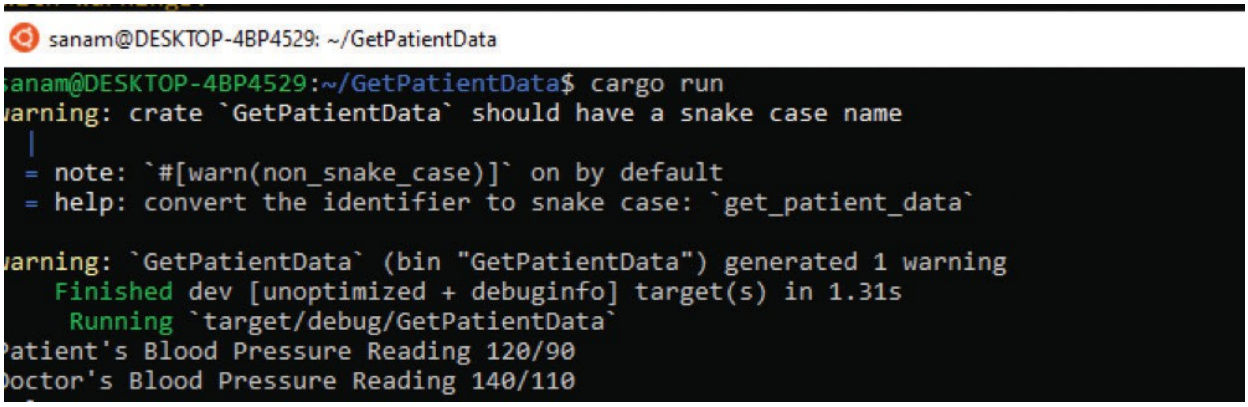

Fig. 18. Captura de pantalla de recogida de datos del proveedor de seguros.

posible; en cambio, este artículo aporta la prueba de viabilidad in vitro. La posibilidad de resolución autónoma de conflictos en la sanidad electrónica descentralizada permite el uso valioso de los datos de salud de la persona en diferentes sectores de forma transparente y fiable. Por último, la implementación del prototipo PoC muestra que el caso en ejecución puede implementarse con las tecnologías descentralizadas de vanguardia actuales.

Nuestra investigación se basa en el trabajo de Narendra y colegas,[11]donde los autores proponen la resolución de conflictos con negociación dependiendo del tipo de conflicto. Este estudio proporciona el marco para participantes autónomos unidos en Empresas Virtuales (EV) que propone la estructura en capas presentando diferentes con-textos de lógica empresarial. La investigación muestra que los conflictos se producen en la capa interorga-nizacional, externa. Nuestro trabajo adapta el enfoque definido en la Ref. 11 al ámbito de la sanidad electrónica. El caso de uso de la sanidad confirma que los conflictos se producen en la capa de colaboración interorganiza-cional porque las diferentes partes interesadas pueden tener datos de sanidad electrónica que difieren entre sí. Además, las decisiones empresariales de cada parte interesada pueden diferir de las de los demás, ya que todos los participantes tienen sus propios procesos internos.

Stahnke y sus colegas[80]afirman que la tecnología blockchain permite la aplicación de flujos de trabajo interorganizativos. Para establecer flujos de trabajo fiables y aceptables para todas las partes implicadas en los procesos interorganizativos, es necesario diseñar y validar estos flujos de trabajo utilizando CPN antes de convertirlos en contratos inteligentes. Aunque la CPN se emplea para validar los procesos interorganizativos, es importante reconocer el requisito de que los contratos inteligentes sean legalmente relevantes y cuenten con el apoyo necesario.

Un estudio de Park y sus colegas[81]sugiere incorporar sistemas de planificación de recursos empresariales (ERP) al modelo de simulación de procesos empresariales para utilizar datos reales en el proceso de simulación diseñado por la CPN. Park y van der Aalst[81]pretenden superar la complejidad de los sistemas ERP implantando un marco que permita integrarlos en los procesos de simulación. Sin embargo

difieren de este enfoque, ya que nos abstenemos de introducir componentes de la vida real en la simulación debido a la naturaleza sensible de los datos de e-salud. Además, suponemos que un número ilimitado de partes interesadas y sus sistemas internos participan en procesos interorganizativos de salud electrónica. Por consiguiente, la integración de sistemas individuales no aporta ningún valor adicional.

En su trabajo, Jadav y sus colegas[82]se centraron en el uso de la IA para descubrir ataques de wearables y compartir datos sanitarios con una blockchain pública. Los autores proponen el uso de la tecnología blockchain para la inmutabilidad de los datos. En nuestra investigación, también afirmamos que la tecnología blockchain permite la inmutabilidad de los datos de salud electrónica, pero no nos centramos en el uso de la IA para descubrir la manipulación de datos. Aun así, el diseño del proceso interorganizacional propuesto en este artículo permite integrar actores no humanos, como los agentes de IA.

El marco DeepBlockShield propuesto por Kim y Kim[83]pretende resolver los problemas de fuga de datos médicos con la tecnología blockchain. La solución correspondiente propone almacenar los datos en una cadena de bloques y proporcionar acceso a agentes especiales. En nuestra investigación, partimos de la base de que los datos médicos pueden almacenarse no solo en una cadena de bloques y proponemos el marco MFSSIA para establecer una colaboración segura entre las distintas partes interesadas a la hora de compartir los datos de salud electrónica.

Un estudio reciente de Abbas y sus colegas[84]propuso un marco para compartir y acceder de forma segura a los datos de dispositivos portátiles, utilizando la tecnología blockchain para garantizar la seguridad de la transmisión de datos y la gestión entre nodos interconectados. Los autores han evaluado la eficacia de los resultados de su investigación en términos de exactitud, ratio de precisión, valor medio de confianza y tiempo de respuesta. En nuestra investigación, empleamos las herramientas formales CPN para evaluar el proceso de diseño y garantizar que no haya problemas de diseño. Además, nuestro proceso de diseño hace hincapié en la resolución de los conflictos de procesamiento de datos, además de abordar los problemas de seguridad.

Este artículo se centra principalmente en los aspectos técnicos de la implementación de blockchain en la gestión de datos de healthcare

específicamente en la integración de datos personales y de HCE. Dada esta orientación técnica, este estudio no implica directamente a sujetos humanos ni recoge datos en los que la raza o la etnia sean factores relevantes.

En casos como estos, en los que la investigación se centra en el desarrollo tecnológico y no en los seres humanos, no es aplicable recopilar datos sobre raza o etnia. Nuestro estudio se centra más en los retos y soluciones sistémicos y tecnológicos de la integración de datos sanitarios que en las características demográficas de los usuarios finales. Sin embargo, en el contexto más amplio del despliegue, estos factores influyen en la implantación de la tecnología sanitaria y en sus repercusiones sociales.

Conclusiones

En este artículo, investigamos la resolución automática de conflictos en sistemas sanitarios electrónicos descentralizados con tecnología blockchain. Esta última permite procesos interorganizativos autónomos y transparentes y un mecanismo fiable de resolución de conflictos sin la intervención de una autoridad central. Nuestro enfoque propuesto se basa en varios métodos científicos, como DSR, modelado CPN y marcos, como T-DM, eSourcing y MFSSIA. Utilizamos T-DM para la definición de los requisitos de un sistema basado en blockchain con el fin de sentar las bases para el diseño de la arquitectura del sistema, la economía de fichas que define los conjuntos de transacciones en la cadena y el desarrollo de protocolos dinámicos. Además, mapeamos los objetivos funcionales definidos por T-DM en los que se producen conflictos a las nociones de proceso BPMN. Por último, evaluamos los resultados de nuestra investigación con CPN, ya que valida los conceptos de resolución de conflictos definidos con T-DM en el proceso en ejecución. Nuestra evaluación incluye una implementación prototipo PoC del caso en ejecución. Tanto con la evaluación PoC de la CPN como con la del prototipo, garantizamos que la investigación puede utilizarse en procesos en tiempo real.

Proponemos utilizar una DAO como solucionador automático de conflictos a la hora de procesar y mapear datos personales de salud electrónica en procesos interorganizativos. Los requisitos para la resolución automática de conflictos son la creación d e datos PHR y EHR por varias partes interesadas en el entorno descentralizado. Dichas partes interesadas se incorporarán y autenticarán con MFFSIA para acordar el uso compartido de datos de salud electrónica y las técnicas de resolución de conflictos de uso utilizadas por una DAO. Los datos de salud electrónica procedentes de distintas fuentes se fusionarán antes de su utilización. Tras definir los requisitos para la recopilación y el procesamiento de datos de salud electrónica, proponemos dos tipos de conflictos: la regla de negocio interno y los conflictos por diferencias de datos. Por último, proponemos que, en caso de conflicto de diferencia de datos, el sistema descentralizado vuelva a comprobar los datos mediante varios nodos y decida qué datos son correctos.

Nuestra investigación tiene varias limitaciones. En primer lugar, tenemos que evaluar exhaustivamente la MFSSIA integrada en el contexto de los procesos de intercambio de datos entre organizaciones. Además, este estudio

Además, este estudio no ha definido en profundidad los retos específicos a los que se enfrenta la implantación de sistemas de sanidad electrónica. Por otra parte, el concepto de economía de fichas, que implica el reparto de los ingresos de la comunidad entre los productores de contenidos y los usuarios de servicios que aportan valor, queda fuera del alcance de este trabajo. Por consiguiente, los aspectos de la economía de fichas y los costes de transacción no se abordan en nuestra investigación.

Preservar la privacidad de los datos de los usuarios es de suma importancia, ya que no hacerlo puede tener implicaciones legales. Sin embargo, este estudio no explora los aspectos legales relacionados con la protección de la privacidad de los datos de los usuarios. Por lo tanto, la aceptación y aplicación de las técnicas propuestas dependen de la jurisdicción legal del país y del cumplimiento por parte del hospital de las leyes y normativas pertinentes.

Trabajamos en las reglas del conjunto de retos específicos de la sanidad electrónica para la MFSSIA. Tras implementar un prototipo PoC, planeamos colaborar con proveedores sanitarios para probar los resultados de nuestra investigación con casos de uso reales. Asimismo, el trabajo futuro está relacionado con la resolución de los retos asociados a la heterogeneidad del entorno socioadministrativo. En el diseño propuesto, definimos acuerdos entre las partes interesadas con contratos inteligentes inmutables. El trabajo futuro está relacionado con la superación de este reto con el desarrollo del ciclo de vida de los contratos inteligentes de e-salud que permite la adopción de los cambios en los acuerdos de la vida real a los definidos por los contratos inteligentes.

Por último, la interoperabilidad de los datos de la sanidad electrónica es uno de sus mayores retos. El uso de normas comunes, como SNOMED CT, HL7, LOINC, etc., pretende resolver este problema. Al mismo tiempo, como consideramos que el proceso interorganizativo es flexible y admite un número ilimitado de partes interesadas, se plantean retos relacionados con la privacidad de los datos y la interoperabilidad. Partimos de la base de que tanto los participantes humanos como los no humanos en el contexto M2X deben autenticarse en el marco MFSSIA para acceder a dichos procesos. Dado que MFS-SIA utiliza conjuntos de retos y autenticación de identidad basada en respuestas, los estándares de datos de salud electrónica compatibles pueden formar parte de los conjuntos de retos que se desarrollen en el futuro. El trabajo futuro también incluye la adopción de agentes de IA que puedan utilizarse en diferentes fases de procesos interorganizativos, como la autenticación MFSSIA, la recopilación de datos de e-salud y la resolución de conflictos, con más por venir.

Financiación

Sin financiación.

Relaciones y actividades financieras y no financieras

El Dr. Norta es miembro del Consejo Editorial de BHTY; no hay otras declaraciones que comunicar.

Colaboradores

Todos los autores han contribuido a este artículo. Aleklsandr Kormilt-syn escribió el artículo y realizó la investigación. Alex Norta supervisó el artículo y aportó sus comentarios. Chibuzor Udokwu y Vimal Dwivedi editaron el artículo y aportaron sus comentarios. Sanam Nisar desarrolló un prototipo de prueba de concepto.

Referencias

1. Susskind RE, Susskind D. El futuro de las profesiones: cómo la tecnología transformará el trabajo de los expertos humanos. Oxford University Press; 2015.
2. Mercille J. Privatización en el sector hospitalario irlandés desde 1980. J Public Health. 2018;40:863-70. https://doi.org/10.1093/pubmed/ fdy027
3. Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus SE. Registros personales de salud: una revisión de alcance. J Am Med Inform Assoc. 2011;18:515-22. https://doi.org/10.1136/amiajnl-2011-000105
4. Levitan B, Getz K, Eisenstein EL, Goldberg M, Harker M, Hes-terlee S, et al. Evaluación del valor financiero de la participación de los pacientes: un enfoque cuantitativo del proyecto Grupos de Pacientes y Ensayos Clínicos de CTTI. Ther Innov Regul Sci. 2018;52:220-9. https://doi.org/10.1177/2168479017716715
5. Dimitrov DV. Internet médico de las cosas y big data en la atención sanitaria. Healthc Inform Res. 2016;22:156-63. https://doi.org/10.4258/hir.2016.22.3.156
6. Korniltsyn A, Udokwu C, Karu K, Thangalimodzi K, Norta A. Mejora de los procesos sanitarios con contratos inteligentes. En: Proceedings of the international conference on business informa-tion systems. Springer, 2019; pp. 500-13.
7. Norta A, Hawthorne D, Engel SL. A privacy-protecting da-ta-exchange wallet with ownership-and monetization capabili-ties. En: Actas de la Conferencia conjunta internacional sobre redes neuronales 2018 (IJCNN). IEEE, 2018; pp. 1-8.
8. Eccher C, Piras EM, Stenico M. TreC - a REST-based Regional PHR. User Centred Networked Health Care A. Moen et al. (Eds.) IOS Press, 2011. https://doi.org/10.3233/978-1-60750-806-9-108
9. Urbauer P, Sauermann S, Frohner M, Forjan M, Pohn B, Mense A. Aplicabilidad de los componentes IHE/Continua para los sistemas PHR: aprender de las experiencias. Comput Biol Med. 2015;59:186–93. https://doi.org/10.1016/j.compbiomed.2013.12.003
10. Zhang R, Liu L. Security models and requirements for healthcare application clouds.I n Proceedings of the 2010 IEEE 3rd Interna-tional Conference on Cloud Computing. IEEE, 2010; pp. 268-75.
11. Narendra NC, Norta A, Mahunnah M, Ma L, Maggi FM. Sound conflict management and resolution for virtu-al-enterprise collaborations. Serv Oriented Comput Appl. 2016;10:233-51. https://doi.org/10.1007/s11761-015-0183-0
12. Szabo N. Contratos inteligentes: bloques de construcción para los mercados digitales. EXTROPY J Transhumanist Thought. 1996;18:2.
13. Unión Europea. Carta de los derechos fundamentales de la Unión Europea [Internet]. Europa.eu; 2012 [citado 2023 Jun 15]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=celex:12012P/TXT
14. Cláusulas Contractuales Tipo (CCC) [Internet]. Comisión Europea. [citado 2023 Jun 15]. Disponible en: https://ec.europa.eu/info/law/law-topic/ data-protection/international-dimension-data-protection/ standard-contractual-clauses-scc_en
15. Introducción a la función hash como técnica de seudonimización de datos personales. Supervisor Europeo de Protección de Datos [Inter-net]. edps.europa.eu. 2023 [citado 2023 Nov 15]. Disponible en: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_es
16. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. Seguridad y privacidad en el internet médico de las cosas: una revisión. Secur Commun Netw. 2018;2018:5978636. https://doi. org/10.1155/2018/5978636
17. Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. Cuestiones de ciberseguridad y privacidad para aplicaciones de salud móvil socialmente integradas que operan en un en-torno multi-nube. Health Inform J. 2019;25:315-29. https://doi. org/10.1177/1460458217706184
18. Katurura M, Cilliers L. A review of the implementation of elec-tronic health record systems on the African continent. En: Pro-ceedings of the African Computer and Information System & Technology Conference. 2017; pp. 10-11.
19. Cilliers L. Wearable devices in healthcare: privacy and informa-tion security issues. Health Inf Manag J. 2019;49(2-3):150-6. https://doi.org/10.1177/1833358319851684
20. Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiquz-zaman M. Privacyprotector: privacy-protected patient data col-lection in IoT-based healthcare systems. IEEE Commun Mag. 2018;56:163–8. https://doi.org/10.1109/MCOM.2018.1700364
21. Hussein AF, ArunKumar N, Ramírez-González G, Ab-dulhay E, Tavares JMR, de Albuquerque VHC. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet trans-form. Cogn Syst Res. 2018;52:1-11. https://doi.org/10.1016/j. cogsys.2018.05.004
22. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. Fhir-chain: aplicando blockchain para compartir datos clini-cos de forma segura y escalable. Comput Struct Biotechnol J. 2018;16:267-78. https://doi.org/10.1016/j.csbj.2018.07.004
23. Azorín-López J, Fuster-Guillo A, Saval-Calvo M, Bradley D. Tecnologías domésticas, sistemas inteligentes y eSalud. En: Futuros mecatrónicos. Springer, 2016; pp. 179-200.
24. Dittmar A, Meffre R, De Oliveira F, Gehin C, Delhomme G. Dispositivos médicos vestibles que utilizan tecnologías textiles y flexibles para la monitorización ambulatoria. En: Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference. IEEE, 2006; pp. 7161-4.
25. Sebestyen G, Hangan A, Oniga S, Gál Z. eHealth solutions in the context of Internet of Things. En: Actas de la Conferencia Internacional 2014 del IEEE sobre Automatización, Calidad y Pruebas, Robótica. IEEE, 2014, pp. 1-6.
26. Salehi S, Giacalone M. Conflict resolution with equitative algo-rithms: a tool to establish a European common ground of avail-able rights. En: F. Romeo, S. Martuccelli & M. Giacalone (Eds.). The European common ground of available rights. Nápoles: Edi-toriale Scientifica; 2009, p.111.
27. Xu H, Hipel KW, Kilgour DM, Fang L. Resolución de conflictos utilizando el modelo gráfico: interacciones estratégicas en competencia y cooperación. Springer, 2018.
28. Neyens G. Gestión de conflictos para sistemas autónomos. En: Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, 2017; pp. 369-70.
29. Priya KF, Patil NN. Resolving privacy conflict for main-taining privacy policies in online social networks. Int J Com-put Eng Technol. 2019;10:94–101. https://doi.org/10.34218/ IJCET.10.3.2019.011
30. Hölbl M, Kompara M, Kamišalić, A, Nemec Zlatolas L. A sys-tematic review of the use of blockchain in healthcare. Symmetry. 2018;10:470. https://doi.org/10.3390/sym10100470

31. Agbo CC, Mahmoud QH, Eklund JM. Tecnología blockchain en la asistencia sanitaria: una revisión sistemática. En: Actas de la atención sanitaria. Instituto multidisciplinar de edición digital, 2019; Vol. 7, p. 56.
32. McGhin T, Choo KKR, Liu CZ, He D. Blockchain en aplicaciones de atención médica: desafíos y oportunidades de investigación. J Netw Comput Appl. 2019;135:62-75. https://doi.org/10.1016/j.jnca.2019.02.027
33. Swan M. Blockchain: blueprint for a new economy. O'Reilly Media, Inc; 2015.
34. Buterin V. A next generation smart contract & decentralized ap-plication platform. Whitepaper. Fundación Ethereum; 2013.
35. Becker G. Esquemas de firma Merkle, árboles merkle y su criptoanálisis. Ruhr-University Bochum, Tech. Rep; 2008.
36. Hevner A, Chatterjee S. Investigación de la ciencia del diseño en sistemas de información. Integrated Series in Information Systems. 2010; pp. 9-22.
37. Westaway MD, Stratford PW, Binkley JM. The patient-specific functional scale: validation of its use in persons with neck dys-function. J Orthop Sports Phys Ther. 1998;27:331-8. https://doi.org/10.2519/jospt.1998.27.5.331
38. Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. J Inf Process Syst. 2018;14:101-28.
39. Bitcoin-Dinero P2P de código abierto [Internet]. bitcoin.org. [citado 2023 jun 15]. Disponible en: https://bitcoin.org
40. Inicio| Ethereum [Internet]. ethereum.org. 2019 [citado 2023 jun 15]. Disponible en: https://www.ethereum.org
41. Hyperledger Fabric-Hyperledger [Internet]. Hyperledger; 2017 [citado 2023 jun 15]. Disponible en: https://www.hyperledger. org/projects/fabric
42. Udokwu C, Kormiltsyn A, Thangalimodzi K, Norta A. The state of the art for blockchain-enabled smart-contract- applica-tions in the organization. En: Actas de la Conferencia Abierta Ivannikov Ispras 2018 (ISPRAS). IEEE, 2018; pp. 137-44.
43. Weyl EG, Ohlhaver P, Buterin V. Sociedad descentralizada: Encontrando el alma de Web3. Disponible en SSRN 4105763 2022.
44. Informe temático [Internet]. Disponible en: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
45. Damjan M. La interfaz entre blockchain y el mundo real. En: Ragion pratica. 2018; pp. 379-406.
46. Caldarelli G, Ellul J. The blockchain oracle problem in decentral-ized finance-a multivocal approach. Appl Sci. 2021;11:7572. https://doi.org/10.3390/app11167572
47. Liu L, Zhou S, Huang H, Zheng Z. From technology to society: an overview of blockchain-based DAO. IEEE Open J Comput Soc. 2021.
48. Grefen P, Aberer K, Hoffner Y, Ludwig H. CrossFlow: cross-organizational workflow management in dynamic virtual enter-prises. Comput Syst Sci Eng. 2000;1:277-90.
49. Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, et al. Smart e-health gateway: bringing intelligence to internet-of-things based ubiquitous health-care systems. En: Actas de la 2015 12th Annual IEEE Con-sumer Communications and Networking Conference (CCNC). IEEE, 2015; pp. 826-34.
50. Leiding B, (sup) Dieter Hogrefe, Clemens HC, Norta A. The M2X economy-business interactions, transactions and col-laborations among autonomous smart devices. Tesis doctoral, Georg-August-Universitaet Goettingen, 2019.
51. Shiang CW, Meyer JJ, Taveter K. Metodología orientada a agentes para el diseño de agentes cognitivos para juegos serios. Ingeniería de sistemas multiagente. 2016; p. 39.
52. Barr ET, Harman M, McMinn P, Shahbaz M, Yoo S. El problema del oráculo en las pruebas de software: un estudio. IEEE Trans Softw Eng. 2014;41:507-25. https://doi.org/10.1109/ TSE.2014.2372785
53. Norta A, Mahunnah M, Tenso T, Taveter K, Narendra NC. An agent-oriented method for designing large socio-technical ser-vice-ecosystems. En: Proceedings of the 2014 IEEE World Con-gress on Services. IEEE, 2014; pp. 242-9.
54. Sherkat M, Mendoza A, Miller T, Burrows R. Emotional at-tachment framework for people-oriented software. arXiv pre-print arXiv:1803.08171 2018.
55. Kormiltsyn A. Un enfoque sistemático para definir los requisitos e ingeniar la ontología para fusionar semánticamente conjuntos de datos para sistemas de salud centrados en las personas. 2018.
56. Sherkat M. Emocionalismo en la ingeniería de software. Tesis doctoral, 2019.
57. Mendoza A, Miller T, Pedell S, Sterling L, et al. El papel de las emociones de los usuarios y los objetivos de calidad asociados en la apropiación de sistemas: dos estudios de caso. En: Proceedings of the 24th Austral-asian Conference on Information Systems. 2013.
58. Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secure Comput. 2004;1:11-33. https://doi. org/10.1109/TDSC.2004.2
59. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. J Big Data. 2018;5:1. https://doi.org/10.1186/s40537-017-0110-7
60. Fulpagare Priya K, Patil NN. Técnicas de detección de conflictos para preservar la privacidad en los medios sociales. 2018.
61. Udokwu C, Norta A. Derivación y formalización de requisitos de aplicaciones descentralizadas para colaboraciones interorganizacionales en blockchain. Arab J Sci Eng. 2021;46:8397-8414. https://doi.org/10.1007/s13369-020-05245-4
62. Jensen K, Kristensen LM. Coloured Petri nets: modelling and validation of concurrent systems. Springer Science & Business Media, 2009.
63. Mahunnah M, Norta A, Ma L, Taveter K. Heuristics for de-signing and evaluating socio-technical agent-oriented behaviour models with coloured petri nets. En: Proceedings of the Computer Software and Applications Conference Workshops (COMP-SACW), 2014 IEEE 38th International. IEEE, 2014; pp. 438-43.
64. Norta A, Kormiltsyn A, Udokwu C, Dwivedi V, Aroh S, Ni-kolajev I. A blockchain implementation for configurable multi-factor challenge-set self-sovereign identity authentication. En: Ezzat SK, Saleh YN, Abdel-Hamid AA (Eds.). Blockchain Ora-cles: state-of-the-art and research directions. IEEE Access; 2022.
65. Riley L. La interoperabilidad DLT universal ya es una realidad práctica. Blog de la Fundación Hyperledger [Internet]. 2021 [citado 2023 Oct 7]. Disponible en: https://www.hyperledger.org/blog/2021/05/10/ universal-dlt-interoperability-is-now-a-practical-reality
66. Kormiltsyn A, Norta A. Dynamically integrating electron-ic-with personal health records for ad-hoc healthcare quality improvements. En: Actas de la Conferencia Internacional sobre Transformación Digital y Sociedad Global. Springer, 2017; pp. 385-99.
67. Norta AH. Exploring dynamic inter-organizational business pro-cess collaboration [Internet]. 2007 [citado el 7 de octubre de 2023]. Disponible en: https://research.tue.nl/files/2003544/200710444.pdf
68. Kormiltsyn A, Norta A. Formal evaluation of privacy-conflict resolution for integrating personal-and electronic health records in blockchain-based systems. Informe técnico. 2022.

69. Norta A, Eshuis R. Specification and verification of harmonized business-process collaborations. Inf Syst Front. 2010;12:457–79. https://doi.org/10.1007/s10796-009-9164-1
70. Zhao F, Xiang D, Liu G, Jiang C. A new method for measur-ing the behavioral consistency degree of WF-net systems. IEEE Trans Comput Soc Syst. 2021;9:480-93. https://doi.org/10.1109/ TCSS.2021.3099475
71. Weidlich M. Behavioural profiles: a relational approach to be-haviour consistency. Tesis doctoral, Universität Potsdam; 2011.
72. Workflow Nets-ML Wiki [Internet]. mlwiki.org. [citado 2023 jul 11]. Disponible en: http://mlwiki.org/index.php/Workflow_Nets
73. Gehlot V, Sloane E, Thalassinidis AE. Personal health technol-ogy: CPN based modeling of coordinated neighborhood care environments (hubs) and personal care device ecosystems. 2019.
74. Jensen K, Kristensen LM, Wells L. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. Int J Softw Tools Technol Transf. 2007;9:213-54. https://doi. org/10.1007/s10009-007-0038-x
75. sanamnisarmalik. sanamnisarmalik/hprivacyconflictresolu-tionbyblockchain [Internet]. GitHub. 2022 [citado 2023 Sep 25]. Disponible en: https://github.com/sanamnisarmalik/ hprivacyconflictresolutionbyblockchain
76. Nisar S. Defining blockchain-based techniques for privacy con-flict-resolution in cross-organizational processes for e-health systems. Tesis de máster, Universidad de Tartu, Facultad de Ciencia y Tecnología, Instituto de Informática; 2022.
77. Blockchains for mass adoption [Internet]. polygon.technology. [citado 2023 Jun 15]. Disponible en: https://polygon.technology
78. Polkadot: Interoperabilidad Web3 | Blockchain descentralizada [Internet]. Red Polkadot. [citado 2023 Oct 4]. Disponible en: https://www.polkadot.network/
79. Substrate And Polkadot | Substrate_ [Internet]. substrate.io. [citado 2023 Jun 15]. Disponible en: https://substrate.io/vision/ substrate-and-polkadot/
80. Stahnke S, Shumaiev K, Cuellar J, Kasinathan P. Enforc-ing a cross-organizational workflow: an experience report. En: Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 21st International Conference, BPMDS 2020, 25th International Confer-ence, EMMSAD 2020, Held at CAiSE 2020, Grenoble, France, June 8-9, 2020, Proceedings 21. Springer, 2020. Springer, 2020;
pp. 85-98.
81. Park G, van der Aalst WM. Towards reliable business process simulation: a framework to integrate ERP systems. In Pro-ceedings of the Enterprise, Business-Process and Information Systems Modeling: 22nd International Conference, BPMDS 2021, and 26th International Conference, EMMSAD 2021, Held at CAiSE 2021, Melbourne, VIC, Australia, June 28-29, 2021, Proceedings. Springer, 2021; pp. 112-27.
82. Jadav D, Jadav NK, Gupta R, Tanwar S, Alfarraj O, Tolba A, et al. A trustworthy healthcare management framework using amalgamation of AI and blockchain network. Mathematics. 2023;11:637. https://doi.org/10.3390/math11030637
83. Kim J, Kim M. DeepBlockShield: blockchain agent-based secured clinical data management model from the deep web en-vironment. Mathematics. 2021;9:1069. https://doi.org/10.3390/ math9091069
84. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Al-mansour FM. Blockchain-assisted secured data management framework for health information analysis.

Apéndice

3-tupla N: Una tupla es una secuencia finita o lista ordenada de números o, más generalmente, de objetos matemáticos, que se denominan elementos de la **tupla**. Una 3-tupla se denomina triple (o triplete). El número n puede ser cualquier número entero no negativo.

Modelización orientada al agente (MOA): Se utiliza en el modelado de organizaciones y sistemas de información para proporcionar descripciones intencionales de procesos como una red de relaciones entre actores. Como tales, capturan y representan objetivos, dependencias, intenciones, creencias, alternativas, etc.

Sistemas algorítmicos de decisión (SAD): delegación de la toma de decisiones y su ejecución en máquinas.

Grafo bipartito: Gráfico en el que los vértices pueden dividirse en dos conjuntos disjuntos, de forma que todas las aristas conectan un vértice de un conjunto con un vértice de otro conjunto.

Modelo y Notación de Procesos de Negocio (BPMN): Representación gráfica para especificar procesos de negocio en un modelo de procesos de negocio.

Modelo de red de Petri coloreada (CPN)[69]: Extensión retrocompatible del concepto matemático de redes de Petri.

Redes de Petri coloreadas (CPN): Amplían el vocabulario de las Redes de Petri ordinarias y añaden características que las hacen adecuadas para modelar grandes sistemas.

Organizaciones Autónomas Descentralizadas (OAD): Entidad en la que todos los miembros participan en la toma de decisiones porque no existe una autoridad central.

Artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea: Según se define en la Carta de los Derechos Fundamentales de la Unión Europea[13]el artículo 7 es el derecho de toda persona a que se respete su vida privada y familiar, su domicilio y su correspondencia.

DeepBlockShield: Un modelo que implementa el intercambio seguro de datos clínicos. Adopta una metodología de verificación bidireccional del usuario y de suministro asíncrono de información para mejorar la seguridad de los datos clínicos.

Ciclos de investigación de la ciencia del diseño: Proceso que incluye seis pasos: identificación y motivación del problema, objetivos de una solución, diseño y desarrollo, evaluación y comunicación.

Investigación en ciencias del diseño (DSR): Investigación que inventa un nuevo artefacto intencionado para abordar un tipo generalizado de problema y evalúa su utilidad para resolver problemas de ese tipo.

Salud electrónica (HCE): Datos de un paciente creados por profesionales sanitarios y almacenados digitalmente.

Planificación de Recursos Empresariales (ERP): Un tipo de software que las organizaciones utilizan para gestionar sus actividades cotidianas y agilizar los procesos empresariales. Los sistemas ERP integran varias funciones de distintos departamentos, como finanzas, recursos humanos, compras, fabricación, gestión de la cadena de suministro, etc., en una única plataforma unificada.

Ethereum mainnet: La principal cadena de bloques pública de producción de Ethereum, donde se producen las transacciones de valor real en el libro mayor distribuido. Ethereum utiliza una prueba de participación (PoS) en la que la validación no se basa en los recursos empleados en la resolución de problemas matemáticos, sino en la reputación de un nodo.

Consejo Europeo de Protección de Datos (CEPD): Organismo independiente de la Unión Europea con personalidad jurídica cuya finalidad es garantizar la aplicación coherente del Reglamento General de Protección de Datos y promover la cooperación entre las autoridades de protección de datos de la UE.

Modelo Gráfico para la Resolución de Conflictos (GMCR): Una herramienta flexible para su uso en la gestión estratégica dentro de un entorno competitivo.

Health Level Seven International (HL7): Una norma de notificación de resultados clínicos que ya es omnipresente en los sistemas sanitarios de todo el mundo.

Modelos de Markov ocultos (HMM): Modelos secuenciales. Es decir, dada una secuencia de entradas, como palabras, un HMM calculará una secuencia de salidas de la misma longitud. Un modelo HMM es un grafo en el que los nodos son distribuciones de probabilidad sobre etiquetas y aristas, que dan la probabilidad de transición de un nodo a otro.

Internet de las Cosas (IoT): La red colectiva de dispositivos conectados y la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos.

Logical Observation Identifiers Names and Codes (LOINC®): Terminología clínica importante para las órdenes y resultados de pruebas de laboratorio y que forma parte de un conjunto de normas designadas para su uso en los sistemas del Gobierno Federal de EE.UU. para el intercambio electrónico de información clínica sanitaria.

Árbol de Merkle o árbol hash: Garantiza que las transacciones almacenadas en una cadena de bloques están correlacionadas mediante hashes matemáticos.

Monedero Metamask: Billetera de criptomoneda de software utilizada para interactuar con la blockchain de Ethereum.

Sistemas multiagente (MAS): Sistema informático compuesto por múltiples agentes inteligentes que interactúan entre sí. Los sistemas multiagente pueden resolver problemas que son difíciles o imposibles de resolver para un agente individual o un sistema monolítico.

Multifactor challenge-set self-sovereign identity authentication (MFSSIA): Permite la interoperabilidad entre cadenas de bloques utilizando oráculos de cadena de bloques.

Paracadenas: Blockchains conectadas a la cadena de retransmisión de Polkadot o Kusama. Son estructuras de datos específicas de la aplicación que validan las transacciones utilizando la cadena de relés, una estructura subyacente que soporta la comunicación segura entre todas las blockchains conectadas, también conocidas como parachains.

Historia clínica personal (PHR): Información electrónica relacionada con la salud de una persona.

Personal Health Token (PHT): Un token de utilidad para el sistema descentralizado de salud electrónica centrado en la persona.

Polkadot: Permite transferencias entre cadenas de bloques de cualquier tipo de datos o activos, no sólo tokens. La conexión a Polkadot permite interoperar con una amplia variedad de cadenas de bloques en la red Polkadot.

Prueba de concepto (PdC): También conocida como prueba de principio, es una realización de un determinado método o idea con el fin de demostrar su viabilidad o una demostración en principio con el objetivo de verificar que algún concepto o teoría tiene potencial práctico. Una prueba de concepto suele ser pequeña y puede estar completa o no.

Algoritmo de consenso Proof-of-work (PoW): Un mecanismo de consenso descentralizado que requiere que los miembros de la red se esfuercen en resolver un número hexadecimal encriptado. La prueba de trabajo también se denomina minería, en referencia a la recepción de una recompensa por el trabajo realizado.

SNOMED CT o SNOMED: Colección de términos médicos sistemáticamente organizada y procesable por ordenador que proporciona códigos, términos, sinónimos y definiciones utilizados en la documentación e informes clínicos.

Ciclo de vida del desarrollo de software (SDLC): Proceso rentable y eficiente en el tiempo que utilizan los equipos de desarrollo para diseñar y crear software de alta calidad. El objetivo del SDLC es minimizar los riesgos del proyecto mediante la planificación anticipada para que el software cumpla las expectativas del cliente durante la producción y más allá.

Fichas "Soulbound" (SBT): Un tipo de ficha que sólo puede ser poseída y transferida por una dirección específica. Esto significa que una vez que se crea un token Soulbound y se asigna a una dirección, no puede ser transferido ni ser propiedad de ninguna otra dirección.

Autoridad Española de Protección de Datos (AEPD): Organismo independiente del Gobierno de España que vela por el cumplimiento de las disposiciones legales en materia de protección de datos de carácter personal.

Cláusulas Contractuales Tipo (CCC): Documentación de la CE; esta actualización es un paso importante para garantizar medidas sólidas y actualizadas de protección de datos en las transferencias transfronterizas de datos.

Gestión de datos de prueba (TDM): Proceso para proporcionar acceso controlado a los datos a equipos modernos a lo largo del ciclo de vida de desarrollo de software (SDLC).

Fichas "soulbound" (SBT) útiles e intransferibles: También llamado "token intransferible", es un tipo de NFT que no puede transferirse ni venderse a otro monedero. Estos tipos de tokens se utilizan a menudo para representar credenciales, afiliaciones, logros o membresías.

WF-nets: Formalización para describir modelos de procesos en sistemas paralelos y distribuidos.