BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

INVESTIGACIÓN ORIGINAL

Soulbound Tokens: Mecanismo de autenticación descentralizado y respetuoso con la intimidad para el almacenamiento de datos médicos

Biagio Boi, PhD , Estudiante; Franco Cirillo, PhD , Estudiante; Marco De Santis, PhD , Estudiante; y Christian Esposito, PhD

Departamento de Informática, Universidad de Salerno, Fisciano, Italia Autor correspondiente:

Franco Cirillo, Correo electrónico: fracirillo@unisa.it

DOI: https://doi.org/10.30953/bhty.v7.334

Palabras clave: autenticación, blockchain, asistencia sanitaria, historial médico, SBT, identidad autosuficiente, Soulbound Token, SSI

Resumen

Contexto: La digitalización del sector sanitario se enfrenta a importantes retos debido a la diversa represen-tación de los datos y su distribución en varios hospitales. Además, la seguridad es una preocupación clave, ya que los datos relacionados con la atención sanitaria están sujetos a las obligaciones legales del Reglamento General de Protección de Datos (RGPD) y a legislación similar sobre protección de datos. Se han puesto en marcha iniciativas de normalización como Health Level Seven (HL7) para mejorar la interoperabilidad de los datos. Sin embargo, la autenticación sigue siendo una cuestión crítica que plantea importantes retos.
Objetivo: Esta investigación pretende mejorar y reforzar el proceso de autenticación introduciendo una novedosa arquitectura para la autenticación descentralizada. Además, propone un nuevo enfoque para la gestión descentralizada de datos, que es crucial para manejar datos médicos sensibles de forma eficiente.
Metodología: La arquitectura propuesta adopta un enfoque centrado en el usuario, utilizando la identidad autosoberana (SSI). Introduce un nuevo tipo de token no fungible (NFT) denominado token soulbound (SBT) en el contexto médico, que facilitará la autenticación de usuarios en distintos hospitales, creando así una federación de instituciones interconectadas.
Resultados: La implementación de la arquitectura propuesta demostró una reducción significativa del tiempo de autenticación en múltiples hospitales. El uso de SBT garantizó una autenticación de usuarios segura y sin fisuras, mejorando la interoperabilidad general del sistema y la seguridad de los datos. El enfoque descentralizado también mitigó los riesgos asociados a los servidores de autenticación centralizados.
Conclusiones: Este estudio presenta con éxito una novedosa arquitectura de autenticación descentralizada para el ámbito sanitario, aprovechando SSI y SBTs. Este enfoque acelera el proceso de autenticación y mejora la seguridad de los datos y la interoperabilidad entre hospitales. La investigación futura deberá explorar la escalabilidad de esta arquitectura y su aplicación en otros sectores que requieran medidas estrictas de seguridad de los datos.

Resumen en lenguaje sencillo

Esta investigación aborda los retos de la sanidad digital, en particular la variedad, distribución y autenticación de datos. Introduce un sistema de autenticación descentralizado que utiliza la identidad autosoberana y un nuevo tipo de fichas no fungibles denominadas soulbound tokens. Este sistema conecta hospitales, reduce los tiempos de autenticación, aumenta la seguridad de los datos y mejora la interoperabilidad de los sistemas. Al descentralizar la autenticación, mitiga los riesgos asociados a los servidores centralizados. Los resultados de este estudio sugieren que este enfoque innovador podría beneficiar a la sanidad y, potencialmente, a otros sectores con necesidades estrictas de seguridad de los datos, aunque se recomienda seguir investigando sobre su escalabilidad y aplicaciones más amplias.

Enviado: 2 de julio de 2024; Aceptado: 9 de agosto de 2024; Publicado: 31 de agosto de 2024

La mejora de la gestión de datos, la eficacia operativa y la atención al paciente dependen de que el sector sanitario se digitalice. Sin embargo, este cambio tropieza con varios obstáculos importantes, sobre todo en lo que respecta a la autenticación y la compatibilidad de los datos. Los datos sanitarios suelen estar dispersos en varios sistemas y organizaciones[1], cada uno de los cuales utiliza un conjunto diferente de normas y tecnologías para gestionar los datos de los pacientes. Esta fragmentación dificulta la integración entre distintos sistemas y provoca discrepancias en la representación de los datos. La ausencia de un formato de datos estándar dificulta el intercambio de datos y aumenta el riesgo de errores e ineficiencias. Como muchos sistemas no siempre funcionan bien juntos, los usuarios pueden tener problemas para acceder fácilmente a sus historiales médicos. Este desorden compromete la eficacia de la coordinación asistencial y podría dar lugar a errores o retrasos en la atención al paciente.

Los métodos convencionales de autenticación sanitaria suelen depender de servidores centralizados para almacenar y validar las credenciales de los usuarios. Estos sistemas centralizados presentan varias dificultades, como:

- Punto único de fallo: Los servidores centralizados utilizados para la autenticación son propensos a fallar. Toda la red puede verse afectada si el servidor falla o se avería, imposibilitando el acceso a los datos de los pacientes por parte del personal de distintas instituciones.
- Problemas de escalabilidad: A medida que las redes sanitarias se desarrollan y su base de usuarios aumenta, los sistemas centralizados pueden no ser capaces de mantener el ritmo de la demanda, lo que podría provocar cuellos de botella en el rendimiento.
- Riesgos relacionados con la ciberseguridad: Los servidores centralizados suelen ser objeto de ciberataques. Si un ataque a estos sistemas tiene éxito, los datos críticos de los pacientes pueden verse comprometidos en violaciones masivas de datos.

La dependencia de sistemas de autenticación centralizados puede dar lugar a graves fallos de seguridad que comprometan la eficacia y seguridad generales de la gestión de datos sanitarios. Esta vulnerabilidad se agrava en un entorno descentralizado en el que los datos están repartidos entre varias instituciones. A los datos sanitarios se les aplican leyes estrictas como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) y el Reglamento General de Protección de Datos (GDPR). Para salvaguardar la privacidad de los pacientes y garantizar su cumplimiento, estas normativas imponen controles estrictos sobre el acceso y la gestión de los datos. Con frecuencia, los métodos de autenticación convencionales no logran alcanzar un compromiso entre la facilidad de uso y la seguridad. Las normas de autenticación complicadas pueden dar lugar a más trabajo administrativo y a posibles incumplimientos. En el caso de los sistemas tradicionales, es difícil garantizar que sólo el personal autorizado acceda a la información importante y, al mismo tiempo, preservar una experiencia de usuario fluida. del usuario.

La complejidad de las redes de datos sanitarios aumenta a la par que el número de usuarios, y las soluciones de autenticación existentes podrían no estar a la altura[(2)]. Varios sistemas convencionales se basan en infraestructuras inflexibles que dificultan su modificación en respuesta a los cambios del sector sanitario o de la tecnología. Es posible que las antiguas técnicas de autenticación queden obsoletas o requieran costosas modificaciones a medida que los sistemas sanitarios se desarrollen e incorporen nuevas tecnologías. Esta falta de flexibilidad y escalabilidad puede dificultar el desarrollo del sector y su adaptación a nuevos problemas.

Esta investigación pretende abordar los retos de autenticación en el sector sanitario proponiendo una novedosa arquitectura de autenticación descentralizada. La solución propuesta aprovecha la identidad autosoberana (SSI), un enfoque centrado en el usuario que potencia el control del individuo sobre sus identidades digitales. Además, la arquitectura introduce un nuevo tipo de token no fungible (NFT) conocido como token soulbound (SBT). Los SBT son un tipo específico de token no transferible introducido para representar credenciales y logros personales en la blockchain de forma segura y verificable.

A diferencia de los tokens fungibles tradicionales o de los NFT transferibles, los SBT están vinculados a una persona concreta y no pueden transferirse ni intercambiarse con terceros. El origen de las SBT radica en la necesidad de un método fiable para representar y verificar digitalmente atributos y credenciales personales como títulos académicos, certificaciones profesionales y registros de afiliación. Esta necesidad se ha hecho más acuciante a medida que la verificación humana adquiere importancia en diversos ámbitos, desde la educación a la creación de redes profesionales, entre otros. El término "soulbound" representa metafóricamente la idea de que estas fichas están intrínsecamente ligadas al "alma" del individuo, es decir, a su identidad personal y única, y no están destinadas a ser separadas o intercambiadas. Al aplicar este enfoque descentralizado, pretendemos crear una red federada de instituciones sanitarias que mejore la seguridad de los datos y la interoperabilidad, al tiempo que reduce significativamente los tiempos de autenticación. Para complementar esta arquitectura de autenticación descentralizada, proponemos la integración de un sistema de gestión de datos Solid (un medio para el intercambio seguro y descentralizado de datos públicos y privados), que proporciona un marco sólido para el almacenamiento y la gestión descentralizados de datos. Al utilizar Solid, los pacientes pueden almacenar sus datos sanitarios personales en almacenes de datos personales en línea (Pods), que controlan totalmente. Esto garantiza que los pacientes tengan la autoridad para conceder o revocar el acceso a su información sanitaria, fomentando la confianza y mejorando la privacidad.[3]

En este informe detallamos la metodología que subyace a la arquitectura propuesta, incluida la integración de SSI y SBT, y presentamos los resultados de nuestra aplicación. Demostramos cómo este enfoque mitiga los riesgos asociados a los servidores de autenticación centralizados y mejora la eficiencia y la seguridad generales del sistema de gestión de datos sanitarios.

Cita: Blockchain en la sanidad hoy 2024, **7**: 334 - https://doi.org/10.30953/bhty.v7.334

la eficacia y la seguridad generales del sistema de gestión de datos sanitarios. Por último, discutimos las implicaciones potenciales de esta arquitectura para la industria sanitaria en general y sugerimos vías para futuras investigaciones.

Antecedentes

En el campo de la gestión de credenciales digitales, la integración de la tecnología blockchain y los protocolos criptográficos ha dado lugar a avances significativos. Un avance destacado es el uso de SBT para emitir y gestionar credenciales de acceso digitales.

Esta sección examina varios enfoques e innovaciones contemporáneos en este ámbito, destacando los puntos fuertes y las limitaciones de cada uno, con especial atención a la privacidad, el no repudio y el cumplimiento de la normativa.

El sistema de gestión de credenciales digitales propuesto en la Ref. 4 introduce un enfoque innovador mediante el aprovechamiento de una versión mejorada de SBTs, denominados tokens rechazables ligados al alma (RejSBTs). Este sistema mejora las características tradicionales de las credenciales incorporando términos y condiciones durante la emisión y garantizando el no repudio de la recepción tras la aceptación por parte de los usuarios. Las RejSBT garantizan el no repudio de las pruebas de recepción y origen, un aspecto crítico a efectos legales y de seguridad. Sin embargo, el protocolo actual carece de medidas de cifrado, ya que maneja principalmente credenciales de acceso digitales no sensibles. Es crucial que las futuras integraciones se ajusten a la normativa GDPR para abordar posibles problemas de privacidad.

Otro enfoque notable es la integración de identificadores descentralizados (DID) con SBT en sistemas de autenticación digital, especialmente en los entornos Web3 y metaverso. Este esquema propuesto por Kim y Ryou (2023)[5]utiliza DIDs para la verificación de usuarios a través de contratos inteligentes y emite SBTs para una integración sin fisuras. Para mejorar la privacidad, los proveedores de servicios de las autoridades de verificación utilizan sistemas de prueba de conocimiento cero (ZKP), garantizando que la información crítica del usuario no se divulgue durante el proceso de verificación. Este método aumenta la conve-niencia del usuario al permitir la generación de pruebas criptográficas sin la participación directa del usuario. Además, un monedero unificado gestiona tanto las credenciales DID como las SBT, lo que simplifica la gestión de credenciales.

En el contexto de los sistemas de credenciales que preservan la privacidad, el uso de SBT combinados con mecanismos de divulgación selectiva está ganando terreno. Un marco[6]propone emitir credenciales como NFT almacenadas en el Sistema Interplanetario de Archivos (IPFS) en un formato cifrado. Aunque este sistema otorga a los usuarios un control total sobre la información de sus credenciales, el proceso de verificación no emplea ZKPs, lo que limita potencialmente sus garantías de privacidad. Un método avanzado para la verificación de identidades privadas[7]implica SBTs de conocimiento-cero, que combinan SBTs con ZKPs. Este protocolo utiliza la clave pública/privada del titular de la identidad para cifrar los datos almacenados en una base de datos pública del titular de la identidad para cifrar los datos almacenados en una SBT. A continuación, se utiliza una ZKP para la verificación, garantizando que los datos no han sido alterados y que el titular de la identidad cumple unos requisitos específicos sin revelar ninguna información personal. Este enfoque equilibra eficazmente la privacidad y la seguridad, lo que lo convierte en una solución sólida para la verificación de la identidad.

El metaverso presenta retos y oportunidades únicos para la gestión de la identidad digital. Una implementación[8]se centra en proporcionar acceso restringido por edad en Decentraland (una plataforma basada en navegador de mundo virtual 3D) utilizando contratos inteligentes Ethereum y ZKPs. Este método permite a los usuarios demostrar su idoneidad para determinadas actividades, como acceder a un cine virtual, sin revelar su identidad real. Aprovecha marcos jurídicos existentes como eIDAS (identificación electrónica) y W3C Verifiable Credentials (credenciales verificables), demostrando la aplicación práctica de la tecnología blockchain para mantener la privacidad al tiempo que se garantiza el cumplimiento de las normas legales.

Un caso práctico de uso de las SBT es la certificación de las vacunas COVID-19. Este sistema propuesto[9]emplea una aplicación descentralizada, en la que las SBT se emiten como fichas intransferibles y revocables, lo que garantiza que se ajustan a la naturaleza intransferible de los registros de vacunación. Aunque este enfoque aborda los aspectos administrativos de la certificación de la vacunación, no aborda explícitamente la privacidad y la confidencialidad, destacando un área para futuras mejoras.

Además, el concepto de descentralización de datos va más allá de la gestión de credenciales y ofrece aplicaciones más amplias en diversos sectores. Un reto importante, aparte de la seguridad, es el almacenamiento de archivos de gran tamaño en la red de cadenas de bloques, ya que las cadenas de bloques tradicionales carecen de capacidad para almacenar archivos de gran tamaño, como imágenes médicas. La integración de soluciones de almacenamiento descentralizadas como IPFS y Solid Pods (almacenes de datos personales que ofrecen un lugar para acceder a los datos, actualizarlos y compartirlos) puede revolucionar la gestión y el intercambio de datos en las redes. Por ejemplo, IPFS proporciona una red de igual a igual para almacenar y compartir datos en un sistema de archivos distribuido, mejorando la disponibilidad de los datos y mitigando el riesgo de puntos centrales de fallo. Un modelo de seguridad propuesto para el almacenamiento de datos en IPFS[10]utiliza la tecnología de compartición de secretos de Shamir (SSS) para cifrar los datos antes de su almacenamiento, implementado en Ethereum y operando sobre un algoritmo de consenso Proof of Work, que requiere una gran potencia de cálculo.

Otro reto del IPFS es que sólo proporciona un hash de los datos, lo que complica la búsqueda de registros de pacientes relacionados. Para resolver este problema, en la Ref. 11, que facilita la búsqueda de datos proporcionando un nombre en lugar de un hash, reduciendo así el tiempo de búsqueda. Así, los sistemas de cadena de bloques se utilizan para almacenar, compartir, utilizar y manipular datos de pacientes. Otra solución es utilizar Solid pods para almacenar datos sanitarios. Ejemplos

Tabla 1. Análisis comparativo de las soluciones de gestión de credenciales Análisis comparativo de las soluciones de gestión de credenciales

Fuente	Características principales	Puntos fuertes	Limitaciones	Privacidad	No repudio	Cumplimiento normativo
Pericàs-Gornals. et al. (2024)[4]	SBTs mejorados con T&C, garantiza el no repudio de la recepción	Garantía legal y de seguridad, no repudio de recepción y origen	Carece de medidas de cifrado, sobre todo para credenciales no sensibles	Bajo	Alta	Necesita una futura adaptación al GDPR
Kim et al. (2023)[5]	DID para verificación de usuarios, ZKP para privacidad, monedero unificado	Mayor privacidad con ZKP, integración sin fisuras	Complejidad de la implementación	Alta	Media	Alineación con las normas legales
Reddy y Kushwaha (2023)[6]	NFT almacenados en IPFS, formato cifrado	Control del usuario sobre la información de credenciales	Falta de ZKP, garantías de privacidad limitadas	Bajo	Media	Necesidad de mejoras de privacidad
Cabot-Nadal et al. (2023)[7]	Combina SBT con ZKP, utiliza clave privada/pública para el cifrado	Equilibra eficazmente privacidad y seguridad	Alta complejidad	Alta	Alta	Fuerte alineación con la normativa sobre privacidad
Zichichi et al. (2023)[8]	Contratos inteligentes Ethereum, ZKPs, eIDAS,W3C VCs	Aplicación práctica en metaversos, mantiene la privacidad y la conformidad	Específico para el acceso con restricciones de edad	Alto	Media	Cumplimiento estricto de las normas legales
Lunesu et al. (2023)[9]	SBT como fichas intransferibles y revocables	Aborda aspectos administrativos	No se centra en la privacidad y la confidencialidad	Bajo	Media	Necesita mejoras para la privacidad
Naz et al. (2019)[10]	IPFS para almacenamiento, SSS para cifrado, consenso PoW	Mayor disponibilidad de datos, mitiga los puntos centrales de fallo	Alta potencia computacional, dificultades de búsqueda	Alta	Media	Gran potencial, pero necesita optimización para la atención sanitaria
Saharan y Prasad (2020)[11]	Facilita la búsqueda de datos con nombres en lugar de hashes	Reduce el tiempo de búsqueda, mejora la compartición y el uso de los datos	Complejidad de la implantación	Media	Media	Fuerte alineación con las normas de gestión de datos
Prop.	Autenticación descentralizada con SBT, cadena de bloques privada (Hyperledger Besu), consenso PoA (QBFT), oráculos de privacidad (Chainlink)	Marco integral, escalable, seguridad mejorada con contratos inteligentes privados	Cadena de bloques privada	Alto	Alta	Fuerte enfoque en el cumplimiento, blockchain privada garantiza la privacidad

DID: identificadores descentralizados; eIDAS: identificación electrónica, autenticación y servicios de confianza; GDPR: Reglamento General de Protección de Datos; IPFS: InterPlanetary File System; NFTs: non-fungible tokens; PoA: Prueba de autoridad; PoW: prueba de trabajo; QBFT: Quorum Byzantine Fault Tolerant; SBTs: soulbound tokens; SSI: Self-Sovereign Identity; SSS: Shamir's Secret Sharing;T&C: terms and conditions;VCs: verifiable credentials W3C:World Wide Web Consortium; ZKP: zero-knowledge proof.

se han publicado su uso y técnicas para optimizar una búsqueda.[12,13] Según la Tabla 1, nuestra solución supera a los métodos existentes al ofrecer un marco completo y escalable que equilibra la privacidad, la seguridad y el cumplimiento normativo. Utiliza la autenticación descentralizada con SBT, una cadena de bloques privada y oráculos que tienen en cuenta la privacidad, lo que garantiza una gran privacidad y seguridad. A diferencia de otros enfoques, aborda limitaciones clave como la falta de cifrado, la complejidad y las restricciones de aplicación, lo que lo convierte en una opción superior y más robusta.

Sistema propuesto

Los avances en los sistemas de gestión de credenciales digitales que utilizan SBT ilustran un progreso significativo en la mejora de la privacidad, la seguridad y la comodidad del usuario. Sin embargo, cada enfoque tiene sus puntos fuertes y sus limitaciones, especialmente en lo que respecta a la preservación de la privacidad y el cumplimiento de la normativa. y el cumplimiento de la normativa. Los avances futuros deben centrarse en la integración de medidas de cifrado sólidas, la protección integral de la privacidad y el cumplimiento de las normas reglamentarias para aprovechar plenamente el potencial de estos sistemas innovadores en la gestión de credenciales digitales.

El estado actual de la técnica pone de manifiesto una importante falta de interoperabilidad entre los datos generados en el ámbito sanitario. Aprovechando normas como HL7, es posible desarrollar soluciones interoperables entre distintos hospitales. Sin embargo, los métodos actuales de almacenamiento de datos, que se basan principalmente en servidores centralizados, requieren un cuidadoso rediseño. Esto incluye revisar los mecanismos de acceso a los datos.

La arquitectura propuesta pretende ofrecer un marco completo para gestionar la autenticación de forma descentralizada, teniendo en cuenta al mismo tiempo las soluciones de datos descentralizados comentadas en la sección anterior.

Cita: Blockchain en la sanidad hoy 2024, **7**: 334 - https://doi.org/10.30953/bhty.v7.334

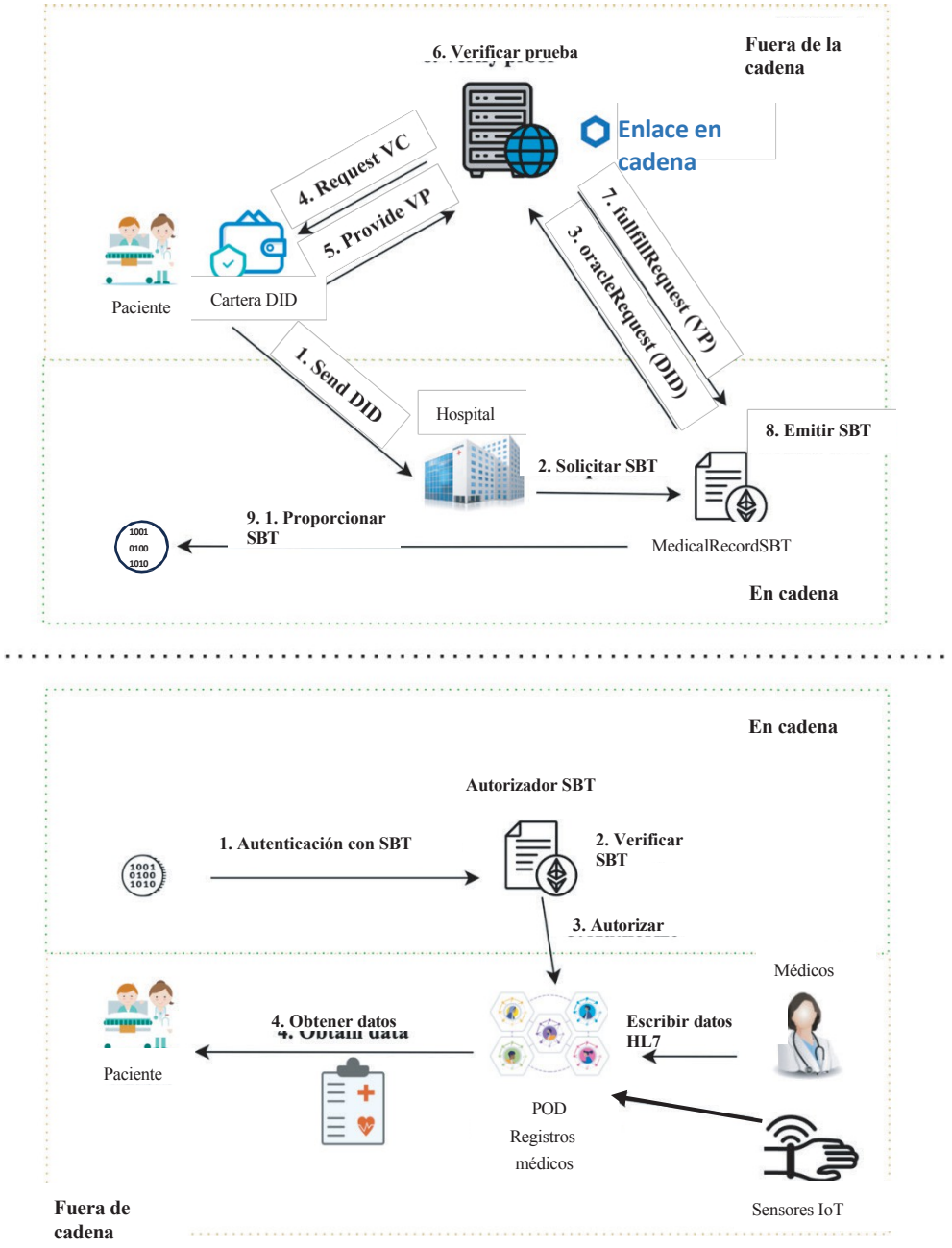

Fig. 1. Modelo de sistema: fase de inscripción (figura superior) y autenticación (figura inferior). HL7: Health Level Seven; IoT: internet de las cosas; Pods: almacenes personales de datos en línea; SBT: soulbound token.

El objetivo es validar este enfoque proporcionando información sobre el tiempo medio de respuesta y una evaluación exhaustiva de la seguridad del protocolo.

Introducción

El uso de DID no es una opción directamente aplicable en el ámbito médico debido a la compleja interacción. Además, la autenticación con SSI plantea importantes retos en las aplicaciones descentralizadas debido al requisito de verificación de la firma de las credenciales, que no puede realizarse en la cadena sin revelar los datos del usuario. Estas preocupaciones se vuelven más críticas cuando se utilizan blockchains públicas como Ethereum.

Nuestra arquitectura pretende ofrecer todas las ventajas de SSI al tiempo que incorpora un novedoso mecanismo de autenticación basado en NFT, concretamente una extensión conocida como Soulbound Tokens (SBT). Los SBT están diseñados para vincular los tokens a su propietario, aprovechando así las ventajas introducidas por las NFT.

Para analizar nuestro sistema, lo dividimos en dos fases principales: la fase de inscripción, representada en la parte superior de la figura 1, y la fase de autenticación, representada en la parte inferior de la figura 2.

parte inferior de la Figura 1. Antes de profundizar en el análisis de estas fases, es necesario aclarar algunos aspectos técnicos relacionados con nuestra arquitectura.

La verificación de credenciales es compleja en la cadena; por este motivo, adoptamos un enfoque híbrido, en el que la identidad se verifica fuera de la cadena y, a continuación, se publica una SBT utilizando una cadena de bloques privada, como Hyperledger Besu. La necesidad de una cadena de bloques privada se debe a la necesidad de garantizar la privacidad del usuario cuando realiza transacciones en la cadena.

Quórum y prueba de autoridad

La arquitectura se ha desplegado en una cadena de bloques privada utilizando Hyperledger Besu, compuesta por cuatro nodos como parte de un proyecto experimental. Esta configuración es fácilmente escalable porque sólo utilizamos blockchain para liberar SBT. En el mecanismo de consenso de Prueba de Autoridad (PoA) empleado, los validadores, que son nodos autorizados a minar bloques, están preautorizados por el propietario de la cadena de bloques.

Cada bloque es validado por uno de estos nodos preautorizados. Hyperledger Besu soporta varios esquemas PoA, incluyendo QBFT, IBFT 2.0 (Istanbul Byzantine Fault Tol-erance), y Clique. Para los propósitos de nuestro proyecto, seleccionamos QBFT debido a su capacidad para garantizar la privacidad de las transacciones, que es esencial para la implementación de un oráculo priva-cy-aware basado en la infraestructura Chainlink. Estas transacciones están protegidas y sólo pueden acceder a ellas las partes implicadas. La escalabilidad de PoA es ventajosa, ya que permite el crecimiento de la red sin problemas significativos de rendimiento. La seguridad y la confianza aumentan porque los validadores son entidades de confianza, lo que reduce el riesgo de actividades maliciosas y garantiza la emisión creíble de SBT. Seleccionamos el esquema QBFT dentro de PoA por sus características de privacidad de las transacciones, cruciales para nuestro oráculo consciente de la privacidad que utiliza la infraestructura Chain-link. En general, la eficiencia, escalabilidad, seguridad y privacidad de PoA lo convierten en la opción ideal para nuestro despliegue de SBT.

Inscripción

La necesidad de una fase de inscripción surge de la com-plejidad de crear un procedimiento oportuno para autenticar a los usuarios dentro del sistema. La autenticación basada en DID requiere la verificación de credenciales y la generación de pruebas verificables por parte del titular, lo que puede introducir sobrecarga. Además, estos procesos no pueden aplicarse a una cadena de bloques pública como la descrita anteriormente.

En nuestra propuesta, la primera fase incluye nueve pasos para entregar una SBT al usuario. Durante esta fase, el usuario comparte las credenciales SSI y recibe una SBT. El procedimiento comienza con la solicitud por parte del titular de una SBT al hospital. Durante esta solicitud, el titular comunica su DID_H, que, en nuestro caso, es un *did:eth* (identificador decen-
(identificador decen- tralizado:Etherium) para garantizar la compatibilidad
compatibilidad con la cadena de bloques de Ethereum. Dicho DID_Hse asocia a un $DIDDocument_H$mediante el uso de el contrato inteligente previamente registrado. El hospital reenvía la solicitud al contrato inteligente MedicalRecordSBT que contiene el mismo DID_H, previamente desplegado en la cadena de bloques de Besu. A continuación, la función requestSBT reenvía esta solicitud a la infraestructura Chainlink, que se encarga de la comunicación fuera de la cadena con el servidor externo. Como se ilustra en la Figura 1, durante los pasos 4, 5 y 6, las solicitudes siguen el enfoque clásico del triángulo de confianza SSI, en el que el verificador, que en este caso es el nodo ChainLink, envía una solicitud al servidor fuera de la cadena, que genera una VPR. Los usuarios generan una presentación verificable conectada a esa VPR y la transmiten al servidor fuera de la cadena, que realiza la verificación de credenciales. Una vez confirmada la validez de las credenciales transmitidas, se ejecuta un call-back en el MedicalRecordSBT, liberando el SBT final al usuario. El usuario puede utilizar ahora esta SBT para autenticarse en plataformas de confianza del hospital.

Autenticación

Al inicio de la autenticación, el paciente ya posee un SBT que representa su identidad dentro del hospital. Este token se utiliza para autenticar al usuario y acceder a los datos personales almacenados en el POD. Todo el procedimiento se gestiona a través del contrato inteligente *SBTAuthorizer*, que contiene referencias al SBT emitido y es capaz de realizar el proceso de autenticación. Este contrato inteligente también incluye metadatos relacionados con los tokens revocados y los roles dentro del sistema, lo que permite al hospital revocar el acceso si un usuario pierde la propiedad de su monedero.

Al igual que los pacientes, los dispositivos del Internet de las cosas (IoT) y los médicos accederán a los espacios de datos utilizando un enfoque descentralizado. Como se describe en la Ref. 14 y en la Ref. 15, tanto los médicos como los dispositivos IoT pueden implementar este tipo de autenticación utilizando SSI. En particular, los médicos gestionarán la autenticación mediante el uso del HSM como mecanismo para reducir el tiempo necesario para la autenticación, mientras que los dispositivos IoT pueden aprovechar las características físicas, como la memoria estática de acceso aleatorio (SRAM), o el electrocardiograma con el fin de crear una clave privada utilizada en la generación del monedero SSI. Por último, la arquitectura propuesta separa el proceso de autenticación del almacenamiento de datos.

Almacenamiento de datos descentralizado

El enfoque propuesto también incluye un novedoso sistema de almacenamiento de datos descentralizado, que es totalmente compatible con el mecanismo de autenticación descentralizado propuesto. Solid, un marco relativamente nuevo, se alinea con el paradigma de almacenamiento de datos centrado en el usuario al permitir a los usuarios asumir la responsabilidad de los datos producidos por las aplicaciones. En este caso concreto, se trata de datos médicos generados tanto por dispositivos IoT como por análisis realizados por médicos. Solid ofrece un método bien estructurado para almacenar datos, utilizando la tecnología de grafos de conocimiento.

Cita: Blockchain en la sanidad hoy 2024, 7: 334 - https://doi.org/10.30953/bhty.v7.334

Tabla 2. Costes de despliegue de la propuesta Costes de implantación de la arquitectura propuesta

Operación	Gas necesario	Coste ($)	Gastado por
Despliegue			
• TokenLink.(constructor)	1467527 gas	11.87	Autoridad
• Operador (constructor)	4184013 gas	33.83	Autoridad
• EthereumDIDRegistry.(constructor)	574518 gas	1.55	Autoridad
• NationalHealthServiceDIDRegistry.(constructor)	1168361 gas	9.45	Autoridad
• MedicalRecordSBT.(constructor)	5159457 gas	41.72	Autoridad
Inscripción			
• EthereumDIDRegistry.updateDIDDocument(cadena,bytes)	742188 gas	6.00	Hospital
• NationalHealthServiceDIDRegistry.authorizeDID(cadena,cadena)	58569 gas	0.47	Hospital
• MedicalRecordSBT.requestSBT(cadena)	164520 gas	1.33	Hospital
Acuñación SBT			
• MedicalRecordSBT.fulfillRequest(cadena)	2594670 gas	20.98	Nodo Chainlink

DID: identificadores/identidad descentralizados; SBT: Soulbound Token.

Esta representación es totalmente compatible con los mecanismos actuales de representación de datos en el ámbito médico, como HL7, que ofrece una ontología bien documentada. Este enfoque mejora el cumplimiento con respecto a GDPR promoviendo el almacenamiento descentralizado de datos, donde los usuarios pueden gestionar los datos producidos por los dispositivos IoT, sin ninguna copia en servidores externos.

Resultados

Para evaluar la calidad de la arquitectura propuesta, nos centramos principalmente en el coste del despliegue de la solución en términos de tarifa por la ejecución de un contrato inteligente. Para la evaluación de nuestra propuesta, desplegamos una imagen Hyper-ledger Besu Docker equipada con QBFT consen-sus sobre un iMac 3.3 GHz Intel Core i5 6 cores equipado con 16 GB 2667 MHz DDR4.

Para implementar nuestras soluciones, hemos desplegado cinco contratos inteligentes:

1. **LinkToken.sol:** Responsable del pago de las solicitudes de Chainlink. Inicialmente desplegado con 1.000.000 LINK.
2. **Operator.sol:** Responsable de operar con el nodo Chainlink, que reenvía todas las peticiones.
3. **EthereumDIDRegistry.sol:** Responsable de gestionar la arquitectura de DIDs.
4. **NationalHealthServiceDIDRegistry.sol:** Responsable de gestionar los roles dentro de todo el marco.
5. **MedicalRecordSBT.sol:** Contiene la definición del SBT y la operación para la acuñación del SBT.

Como se indica en el cuadro 2, el despliegue del contrato inteligente es la operación más costosa, junto con la acuñación del SBT, necesaria para generar y entregar el SBT al usuario. Las solicitudes operativas son necesarias para configurar todo el entorno y hacer referencia a la asignación de los DID creados al registro interno que contiene los roles. La estimación del gas ofrece una idea de la complejidad de las operaciones que implica el contrato inteligente, pero los costes dependerán de múltiples factores, como la ocupación de la red o la tarifa requerida. Asumiendo un coste de 3 gwei por gas necesario, que está en línea con el coste normal de Ethereum block-chain, es posible hacer una estimación sobre el coste total de las diferentes operaciones.

La fase de despliegue se ejecuta una sola vez en el momento de la adopción del sistema, mientras que las operaciones de inscripción y SBT Mint-ing se ejecutan para cada nuevo paciente perteneciente al sistema. Un coste total inferior a 30 dólares por usuario nuevo en el sistema es razonable para las ventajas que introduce el enfoque propuesto.

El procedimiento de autenticación, que sólo consiste en leer datos de la blockchain, no tiene ningún coste adicional.

El tiempo total para el procedimiento de inscripción es de unos 16,03 s de media; la mayor parte se dedica a verificar credenciales (12,54 s). Esta es la principal motivación que nos ha llevado a adoptar un enfoque totalmente descentralizado y en la cadena. Con nuestra propuesta, es posible autenticar ahora utilizando la SBT y comprobando únicamente la presencia de la SBT en el contrato inteligente MedicalRecordSBT.

Con la investigación actual, intentamos reducir el tiempo total necesario para la autenticación proporcionando un método de verificación en la cadena, preservando al mismo tiempo la privacidad de los nodos y todas las ventajas introducidas por SSI. La sobrecarga introducida por la arquitectura propuesta es relativamente baja, teniendo en cuenta que la fase de inscripción se ejecuta una sola vez para cada usuario, y la fase de autenticación se reduce a una única llamada al contrato inteligente. Además, el sistema se basa estrictamente en la cadena de bloques y en el mecanismo asimétrico subyacente a la cadena de bloques. Los SBT aumentan la seguridad aprovechando un monedero criptográfico, que almacena la clave privada asociada a la pública.

Conclusión

En el futuro, tenemos previsto mejorar nuestra evaluación de los métodos propuestos integrando el acceso de los proveedores en escenarios reales. Al incorporar el acceso de los proveedores, podremos simular entornos más complejos y con múltiples partes interesadas, lo que ofrecerá una evaluación más completa de la eficacia de nuestro enfoque en la práctica. Esto nos permitirá comprender mejor el impacto en el mundo real sobre la seguridad y la privacidad de los datos médicos. Por ejemplo, en un caso de uso de la diabetes, el acceso de los proveedores permitiría a los profesionales sanitarios interactuar directamente con los datos de los pacientes almacenados en los Solid Pods y, al mismo tiempo, contribuir y beneficiarse de un modelo de aprendizaje automático distribuido. Esta capa añadida de interacción con el proveedor es esencial para validar la escalabilidad y viabilidad de nuestra arquitectura en varios casos de uso médico.

Financiación

Este trabajo fue parcialmente apoyado por el proyecto SERICS (PE00000014) bajo el programa NRRP MUR financiado por la UE-NGEU y por el proyecto "DHEAL-COM-Digital Health Solutions in Community Medicine" bajo el programa Innovative Health Ecosystem (PNC)-National Recovery and Resilience Plan (NRRP) financiado por el Ministerio de Sanidad italiano.

Conflictos de intereses

Ninguno declarado por los autores.

Colaboradores

El Sr. Boi contribuyó a la conceptualización del sistema, la evaluación del sistema y la redacción. El Sr. Cirillo contribuyó a la conceptualización del sistema, al estado de la técnica y a la redacción general del artículo. El Sr. De Santis contribuyó a la conceptualización del sistema y a la redacción del documento. El Dr. Esposito contribuyó a la conceptualización del sistema y a la revisión de cada borrador.

Todos los autores han aprobado el manuscrito y están de acuerdo con su envío a Blockchain in Healthcare Today.

Declaración de Disponibilidad de Datos (DAS), Intercambio de Datos, Reproducibilidad y Repositorios de Datos.

Póngase en contacto con el autor.

Aplicación de texto generado o tecnología relacionada

En la elaboración de este artículo no se ha utilizado inteligencia artificial ni tecnologías afines.

Agradecimientos

Este trabajo ha sido financiado en parte por el proyecto SERICS (PE00000014) en el marco del programa NRRP MUR financiado por la UE-NGEU y por el proyecto "DHEAL-COM-Digital Health Solutions in Community Medicine" bajo el programa Innovative Health Ecosystem (PNC)-National Recovery and Resilience Plan (NRRP) financiado por el Ministerio de Sanidad italiano.

Referencias

1. Reegu F, Abas H, Jabbari A, Akmam R, Uddin M, Wu CM, Chen CL, Khalaf O. Interoperability Requirements for Block-chain-Enabled Electronic Health Records in Healthcare: A Sys-tematic Review and Open Research Challenges. Security and Communication Networks 2022; 2022(1):9227343. https://doi. org/10.1155/2022/9227343
2. Gupta D, Mazumdar N, Nag A, Singh J. Secure data authentication and access control protocol for industrial health-care system. Journal of Ambient Intelligence and Humanized Computing 2023; 14(5):4853-4864. https://doi.org/10.1007/ s12652-022-04370-2
3. Esposito C, Horne R, Robaldo L, Buelens B, Goesaert E. Assessing the solid protocol in relation to security and pri-vacy obligations. Información 2023; 14(7):411. https://doi. org/10.3390/info14070411
4. Pericàs-Gornals R, Mut-Puigserver M, Payeras-Capellá MM, Cabot-Nadal MÁ, Ramis-Bibiloni J. Digital credentials man-agement system using rejectable soulbound tokens. Ann Tele-commun [Internet]. 2024 Apr 23 [citado 2024 Jun 19]; Disponible en: https://link.springer.com/10.1007/s12243-024-01032-6
5. Kim G, Ryou J. Digital Authentication System in Avatar Using DID and SBT. Mathematics. 2023 Oct 22;11(20):4387. https://doi.org/10.3390/math11204387
6. Reddy S, Kushwaha DS. Framework for privacy preserving cre-dential issuance and verification system using soulbound token. Sumathi AC, Yuvaraj N, Ghazali NH, editores. ITM Web Conf. 2023;56:06002.
7. Cabot-Nadal MÀ, Playford B, Payeras-Capellà MM, Gerske S, Mut-Puigserver M, Pericàs-Gornals R. Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs. En: 2023 7th Cyber Security in Net-working Conference (CSNet) [Internet]. Montreal, QC, Canada: IEEE; 2023 [citado 2024 Jun 19]. p. 153-6. Disponible en: https://ieeexplore.ieee.org/document/10339754/
8. Zichichi M, Bomprezzi C, Sorrentino G, Palmirani M. La protección de la identidad digital en el Metaverso: el caso del acceso a un cine en Decentralandia. En: Conferencia internacional sobre la evolución de la teoría del lenguaje. 2023. Disponible en: https://ceur-ws.org/Vol-3460/papers/DLT_2023_paper_13. pdf
9. Lunesu MI, Tonelli R, Pinna A, Sansoni S. Soulbound Token for Covid-19 Vaccination Certification. En: 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) [Internet]. Atlanta, GA, EE.UU.: IEEE; 2023 [citado 2024 Jun 19]. p.
10. Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, et al. A Secure Data Sharing Platform Using Block-chain and Interplanetary File System. Sostenibilidad. 2019 10;11(24):7054. https://doi.org/10.3390/su11247054
11. Saharan R, Prasad R. Tecnología Blockchain para datos sanitarios. Avances en sistemas inteligentes y computación. 2020 2;671-7. https://doi.org/10.1007/978-981-15-6014-9_81
12. Ghayvat H, Zuhair M, Shukla N, Kumar N. Healthcare-CT: Solid PoD and Blockchain-Enabled Cyber Twin Approach.

for Healthcare 5.0 Ecosystems. IEEE internet of things jour-nal. 2024 Feb 15;11(4):6119-30. https://doi.org/10.1109/JIOT.2023.3312448

13. Ragab M, Savateev Y, Oliver H, Tiropanis T, Poulovassilis A, Chapman A, et al. Unlocking the Potential of Health Data with Decentralised Search in Personal Health Datastores. 13 de mayo de 2024.
14. Barbareschi M, Boi B, Cirillo F, De Santis M, Esposito C. CSe-curing the Internet of Medical Things using PUF-based SSI Authentication. En Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024) 2024.
15. Boi B, Esposito C. Securing the Internet of Medical Things with ECG-based PUF encryption. IET Cyber-Physical Systems: Theory & Applications 2024.

Apéndice: Definición de acrónimos

DID: identificadores/identidad descentralizada
did:eth: identificador descentralizado:Etherium
$DIDDocument_H$: documento de identidad digital (titular) DID_H: identidad digital (titular)
eIDAS: identificación electrónica, autenticación y Servicios de Confianza.
GDPR: Reglamento general de protección de datos
HIPAA: Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios
HL7: nivel sanitario siete
HSM: módulo de seguridad de hardware
IBFT: tolerancia bizantina a fallos de Estambul
IoT: internet de las cosas
IPFS: sistema de archivos interplanetario
NFT: token no fungible
PoA: prueba de autoridad
Pod: almacén personal de datos en línea
PoW: prueba de trabajo
QBFT: Quorum Byzantine Fault Tolerant
RejSBTs: tokens rechazables con alma SBT: token con alma
SRAM: memoria estática de acceso aleatorio SSI: identidad autosuficiente
SSS: Shamir's Secret Sharing (Compartición de secretos de Shamir)
T&C: terms and conditions (Términos y condiciones) VC: verifiable credentials (Credenciales verificables)
VPR: solicitud de presentación verificable
W3C: Consorcio World Wide Web ZKP: zero-knowledge proof (prueba de conocimiento cero)