Cuadernos de Ingeniería. Nueva Serie. Revista de la Facultad de Ingeniería
de la Universidad Católica de Salta (Argentina), núm. 16, 2025

Privacy coins y gestión de historias clínicas: mapeo sistemático de la literatura

Privacy coins and electronic health record management: a systematic mapping study

Guillermina Rosana Nievas[1,2] y Mario Matías Urbieta[3]

Ingeniería en Informática/ artículo de revisión

Citar: Nievas, G. R. y Urbieta, M. M. (2025). *Privacy coins* y gestión de historias clínicas: mapeo sistemático de la literatura. *Cuadernos de Ingeniería* (16). http://revistas.ucasal.edu.ar

Recibido: mayo/2025
Aceptado: agosto/2025

Resumen

La digitalización de las historias clínicas es clave para optimizar la eficiencia y calidad de la atención médica, aunque la protección de los datos de los pacientes sigue siendo un reto importante. En este sentido, la tecnología *blockchain* ha surgido como una alternativa prometedora para mejorar la seguridad en el ámbito sanitario. Sin embargo, su naturaleza rastreable puede comprometer la privacidad del paciente, especialmente en la gestión de historias clínicas electrónicas. Para abordar este desafío, las denominadas *privacy coins*, que emplean técnicas criptográficas avanzadas como firmas en anillo y pruebas de conocimiento cero, podrían garantizar el anonimato y la protección de los datos. Este estudio analiza si estas tecnologías se están utilizando para mejorar la gestión de historias clínicas en entornos basados en *blockchain*, evaluando su efectividad en la protección de la privacidad, su interoperabilidad y su viabilidad técnica y operativa. Por medio de un mapeo sistemático, se establecieron preguntas de investigación, criterios de búsqueda y selección de artículos. Se obtuvieron 72 estudios, de los cuales 24 fueron incluidos en el análisis. Si bien no se identificaron implementaciones completas en historias clínicas electrónicas, se encontraron modelos que combinan *blockchain* con estas tecnologías descentralizadas para fortalecer la privacidad de los datos médicos. Las *privacy coins* permiten anonimización y control granular

[1] Universidad Abierta Interamericana. Facultad de Tecnología Informática. Centro de Altos Estudios en Tecnología Informática. Buenos Aires, Argentina.

[2] Universidad Católica de Salta. Facultad de Ingeniería. Instituto de Estudios Interdisciplinarios de Ingeniería Salta, Argentina.

[3] Universidad Nacional de La Plata. Facultad de Informática. Laboratorio de Investigación y Formación en Informática Avanzada (LIFIA). La Plata, Argentina.

del acceso, ofreciendo ventajas significativas para la protección de la información. Además, su integración con tecnologías como IoMT, FHIR y contratos inteligentes podría reforzar la seguridad, aunque es fundamental equilibrar protección y usabilidad para su aplicación en el sector salud.

Palabras claves: monedas de privacidad, historia clínica electrónica, e-salud, registro de salud digital.

Abstract

The digitalization of medical records is key to optimizing the efficiency and quality of healthcare, although the protection of patient data remains a major challenge. In this regard, blockchain technology has emerged as a promising alternative to improve security in the healthcare field. However, its traceable nature can compromise patient privacy, especially in the management of electronic medical records. To address this challenge, privacy coins, which employ advanced cryptographic techniques such as ring signatures and zero-knowledge proofs, could ensure anonymity and data protection. This study analyzes whether these technologies are being used to improve medical record management in blockchain-based environments, evaluating their effectiveness in protecting privacy, their interoperability, and their technical and operational feasibility. Through a systematic review, research questions and search and selection criteria for articles were established. 72 studies were obtained, of which 24 were included in the analysis. While no direct implementations of privacy coins in electronic medical records were identified, models were found that combine blockchain with these decentralized technologies to strengthen the privacy of medical data. These coins allow for anonymization and granular access control, offering significant advantages for the protection of information. In addition, their integration with technologies such as IoMT, FHIR and smart contracts could reinforce security, although it is essential to balance protection and usability for their application in the health sector.

Keywords: privacy coins, electronic health records, eHealth, digital health records.

1. Introducción

La privacidad en el sector salud representa un desafío crítico en la actualidad. El avance de la digitalización, como la adopción de historias clínicas electrónicas y la expansión de la telemedicina, ha incrementado la exposición del sector a ciberataques. Estos riesgos incluyen la filtración de datos sensibles, *ransomware* y el secuestro de sistemas, comprometiendo no solo infraestructuras críticas sino también la seguridad y privacidad de los pacientes. Ejemplos como el ataque de WannaCry en 2017, que afectó al Servicio Nacional de Salud del Reino Unido con la cancelación de 19 000 citas y pérdidas económicas millonarias, o el ciberataque al Hospital Universitario de Düsseldorf en 2020, que resultó en la muerte de una paciente, evidencian las consecuencias devastadoras de estas amenazas (SeguriLatam, 2022). En Argentina, entre el 30 % y el 40 % de las organizaciones de atención médica han sido víctimas de ciberataques, comprometiendo tanto la privacidad de los pacientes como la operatividad de los sistemas esenciales (Todo Noticias [TN], 2024) .

Ante la creciente sofisticación de los ciberataques, las medidas tradicionales de seguridad son insuficientes. Esto ha impulsado la búsqueda de nuevas tecnologías para garantizar la

protección de los datos clínicos y preservar la confianza pública (Shrivastava y Srikanth, 2022). La implementación de soluciones avanzadas, como *blockchain*, permite registrar información de manera descentralizada, confiable y segura, lo que marca una evolución hacia lo que se denomina *Healthcare 5.0* (Kumar Dubey et al., 2024). Sin embargo, estos avances también presentan desafíos, especialmente en términos de privacidad y confidencialidad.

Los problemas de privacidad, como los identificados en Bitcoin, destacan la vulnerabilidad de las interacciones entre usuarios, la identificación de relaciones y la exposición de identidades reales (Ghesmati et al., 2022). Por medio de metodologías como la *Privacy Risk Analysis Methodology* (PRIAM) se ha modelado el impacto de los riesgos en la privacidad de datos médicos, evidenciando que las brechas de seguridad pueden derivar, además, en daños graves como discriminación, extorsión y daño emocional (Wairimu y Fritsch, 2022).

En este contexto, han surgido dos enfoques principales para abordar los problemas de privacidad: la privacidad adicional (*add-on data privacy*), que mejora los sistemas mediante técnicas complementarias, como la combinación de privacidad diferencial y pruebas de conocimiento cero o ZKP (*Zero Knowledge Proof*) para consultas seguras (Munilla Garrido et al., 2022), y la privacidad integrada (*built-in data privacy*), donde la tecnología es diseñada desde el inicio con características inherentes de privacidad. Un ejemplo clave de esta última son las *privacy coins* (monedas de privacidad), como Monero y ZCash, que emplean técnicas avanzadas de anonimización y ofuscación para proteger la identidad de los usuarios y garantizar transacciones seguras y confidenciales (Ballandies et al., 2022) .

Monero emplea firmas de anillo para garantizar la privacidad de sus transacciones. Esta tecnología criptográfica permite que cualquier miembro de un grupo (el "anillo") firme un mensaje, haciendo imposible determinar quién lo firmó en realidad. En el contexto de Monero, cada transacción se firma utilizando un anillo compuesto por la salida que se desea gastar y múltiples salidas "fantasma" de otros usuarios. Al crear esta firma, se genera una estructura matemática compleja que vincula todas las salidas del anillo, pero sin revelar cuál fue la utilizada específicamente. Esto dificulta enormemente el seguimiento del origen en la *blockchain*, proporcionando un alto nivel de anonimato a los usuarios. Zcash utiliza "pruebas de conocimiento cero" para ocultar información sobre algunas transacciones. En criptografía, una prueba de conocimiento cero es un método que permite a una persona demostrar a otra que conoce un valor específico (por ejemplo, una clave privada), sin revelar ninguna otra información sobre ese valor. En Zcash, estas pruebas se utilizan para ocultar los remitentes, los destinatarios y los importes de las transacciones seleccionadas. De esta manera, se logra un alto nivel de privacidad para los usuarios que optan por utilizar esta función, manteniendo al mismo tiempo la transparencia y la seguridad de la *blockchain* (Akcora et al., 2022) .

Estas tecnologías no solo aseguran la integridad de los datos, sino que también fortalecen la confidencialidad, lo que resulta crucial en entornos donde la privacidad es prioritaria, como el intercambio de información médica o la gestión de registros clínicos sensibles. Así, las *privacy coins* emergen como herramientas esenciales para proteger la identidad de los participantes en sistemas sanitarios, garantizando un equilibrio entre transparencia y privacidad en la era digital.

2. Desarrollo

2.1. Preguntas de investigación

La primera etapa del mapeo sistemático llevado a cabo fue la definición de las preguntas de investigación y su motivación.

Tabla 1. Preguntas de investigación y motivación

Pregunta de investigación	Motivación
P1. ¿Qué modelos o propuestas de implementación de monedas de privacidad en historias clínicas han sido documentados en la literatura académica?	Conocer si esta tecnología ya fue utilizada en el ámbito clínico.
P2. ¿Qué ventajas ofrecen las monedas de privacidad como mecanismos de protección de datos en el ámbito de la salud?	Si fue utilizada, cuáles fueron las ventajas respecto de la privacidad de los datos clínicos.
P3. ¿Qué trabajos abordaron el almacenamiento de información sanitaria con infraestructuras relacionadas a las monedas de privacidad?	Exponer otras tecnologías que abonen al problema central.

2.2. Métodos de revisión

El presente estudio se desarrolló conforme a la metodología del Mapeo Sistemático de la Literatura (MSL), siguiendo el enfoque propuesto por Kitchenham y Brereton (2013), ampliamente adoptado en investigaciones empíricas dentro del campo de la ingeniería del *software* y disciplinas afines de las ciencias computacionales. Esta metodología proporciona un marco estructurado, transparente y replicable que permite identificar, evaluar e interpretar artículos de investigación relevantes. El proceso se organiza en tres fases principales: (1) **planificación de la revisión**, que implica la formulación de preguntas de investigación claras y pertinentes, el desarrollo de un protocolo que establece los criterios de inclusión y exclusión, las fuentes de búsqueda, las cadenas de búsqueda y los procedimientos de extracción y síntesis de datos; (2) **conducción de la revisión**, que consiste en ejecutar la búsqueda sistemática en bases de datos científicas, identificar y seleccionar estudios **primarios** —aquellos que reportan resultados originales de investigaciones empíricas—, excluyendo los estudios **secundarios** como revisiones sistemáticas previas, resúmenes, opiniones o artículos teóricos sin evidencia empírica directa. En esta fase también se evalúa la calidad metodológica de los estudios incluidos, se extraen los datos relevantes de forma estructurada y se sintetizan los hallazgos mediante técnicas apropiadas de codificación o categorización; y (3) **documentación de la revisión**, donde se elabora el informe final que presenta los resultados, el procedimiento seguido y las conclusiones, validado por revisión entre pares para asegurar la claridad, coherencia y valor científico del estudio. Esta estructura metodológica rigurosa permite garantizar la solidez, la transparencia y la reproducibilidad del proceso de revisión, condiciones esenciales en todo estudio secundario de carácter científico.

2.3. Fuentes

A partir del objetivo planteado, y habiendo definido las preguntas de investigación y su motivación, se determinaron los repositorios de búsqueda de las fuentes. Es así que se decidió enfocar en las siguientes bases de datos: Google Scholar, ScienceDirect, Association for Computing Machinery (ACM), Institute of Electrical Electronics Engineers (IEEE), Sage Journals y SEDICI, el Repositorio Institucional de la Universidad Nacional de La Plata (UNLP).

2.4. Definición de términos

La exploración inicial del tema por medio de diversas lecturas permitió identificar la terminología utilizada para referirse a los conceptos analizados en este estudio. Siguiendo la metodología, se definió la cadena de búsqueda a partir de la definición de los términos principales y alternativos.

Tabla 2. Definición de términos

Términos principales	Términos alternativos
privacy coins	*cryptocurrency-based privacy* *digital privacy currency* *monedas de privacidad*
electronic health records	*medical data privacy* *medical records* *health information system* *healthcare data* *historia clínica electrónica*

2.5. Cadena de búsqueda

La cadena de búsqueda quedó conformada de la siguiente manera:

("privacy coins" OR "cryptocurrency-based privacy" OR "monedas de privacidad" OR "digital privacy currency") AND ("historia clínica electrónica" OR "medical data privacy" OR "electronic health records" OR "medical records" OR "health information system" OR "healthcare data").

2.6. Criterios de inclusión y exclusión

Con la ejecución de la búsqueda de acuerdo con los parámetros establecidos, se aplicaron los criterios de inclusión (I) y exclusión (E) a los artículos encontrados, toda vez que estos respondieran a las preguntas de investigación, serían sometidos a los criterios de inclusión y exclusión que se mencionan en la tabla siguiente:

Tabla 3. Criterios de inclusión y exclusión

Criterios de inclusión	Criterios de exclusión
I1: Artículos en idioma inglés y español	E1: Trabajos para la obtención de título de grado y posgrado u otro que no sean artículos científicos. No se consideran tesinas, tesis de especializaciones, maestrías o doctorados.
I2: Artículos publicados desde el año 2019 a la fecha	E2: Trabajos a los que no se tenga acceso al contenido.
	E3: Artículos cuyo contenido no esté relacionado con el ámbito de la salud, aunque incluyan términos de la cadena de búsqueda sin abordar específicamente la temática de estudio.

2.7. Estudios incluidos y excluidos

Se realizó la búsqueda de trabajos, de acuerdo con la cadena de búsqueda definida y en cada una de las fuentes seleccionadas, los resultados se presentan en la Tabla 4 a continuación:

Tabla 4. Detalle de los resultados de búsqueda

Fuente	ACM	Google Scholar	IEEE	Science Direct	SEDICI	Sage Journals	Total
Secundarios[4]		9					9
E1: Trabajos para la obtención de título de grado y posgrado u otro que no sean artículos científicos		13					13
E2: Trabajos a los que no se tenga acceso al contenido		6		1			9
E3: Artículos cuyo contenido no esté relacionado con el ámbito de la salud, aunque incluyan términos de la cadena de búsqueda sin abordar específicamente la temática de estudio.	4	15					16
Válidos	11	10	3				24
Artículos analizados	15	53	3	1	0	0	72

[4] Secundarios: artículos de revisión de literatura o mapeos sistemáticos.

En resumen, las búsquedas en las diferentes fuentes arrojaron un total de 72 artículos. En un primer filtrado, se analizaron los títulos, resúmenes y palabras claves para distinguir los estudios primarios de los secundarios, lo que resultó en una preselección de 63 artículos primarios. Luego, en un segundo filtrado, se aplicaron los criterios de inclusión y exclusión, obteniendo una muestra final de 24 artículos para el análisis.

3. Resultados

La búsqueda y selección de trabajos permitió obtener un conjunto que representa la tendencia dentro del tema investigado en el periodo establecido en el protocolo, y que permitió responder a las preguntas de investigación.

3.1. ¿ Qué modelos o propuestas de implementación de monedas de privacidad en historias clínicas han sido documentados en la literatura académica?

En la literatura académica acerca de la vinculación de monedas de privacidad en historias clínicas, se han documentado dos propuestas relevantes según los criterios de búsqueda realizados.

El primer estudio, de Pareek et al. (2024), analiza el uso de monedas de privacidad en el contexto de la atención sanitaria, específicamente en la prescripción y consumo de medicamentos, aspectos que conforman una historia clínica. Se considera relevante dado que presenta un caso de uso concreto de *privacy coins* en procesos médicos, evidenciando su aplicabilidad para garantizar anonimato y seguridad en entornos de salud. Su inclusión responde a la intención de identificar antecedentes que aporten al análisis del potencial de estas tecnologías en el manejo de datos médicos sensibles. Este enfoque permite explorar posibilidades de extrapolación hacia sistemas de registros clínicos más amplios, dentro del marco de privacidad y protección de datos. El segundo estudio, de Lee y Song (2021), propone un modelo denominado MEXchange para preservar la privacidad en el intercambio de datos médicos. Este modelo utiliza mecanismos criptográficos similares a los empleados por algunas monedas de privacidad, como *ring signatures* y *stealth addresses*, para garantizar la seguridad y confidencialidad de las transacciones. MEXchange también enfatiza la gestión descentralizada de los datos y la interoperabilidad, lo que resulta relevante en el contexto de la privacidad y la seguridad en la gestión de datos médicos.

Ambos estudios ofrecen perspectivas sobre cómo las monedas de privacidad pueden aplicarse en el ámbito sanitario, particularmente en el manejo y la transmisión de datos médicos, aunque ninguno aborda la totalidad de datos que integra una historia clínica. Esto destaca que la investigación en este campo aún está en etapas incipientes, sin un enfoque claro en la integración de monedas de privacidad en sistemas interoperables de historias clínicas.

3.2. ¿Qué ventajas ofrecen las monedas de privacidad como mecanismos de protección de datos en el ámbito de la salud?

Aunque no se ha identificado una implementación específica de monedas de privacidad en historias clínicas electrónicas, diversos estudios han documentado sus ventajas como mecanismos de protección de datos en el sector de la salud en general. En particular, las monedas de privacidad ofrecen múltiples beneficios en términos de seguridad y privacidad, lo

que las convierte en una opción interesante para el manejo de datos sensibles en sistemas de salud. A continuación, se detallan las principales ventajas, según los trabajos de Bernal Bernabe et al. (2019) y Saroop (2024):

1. Anonimización robusta de transacciones: Las monedas de privacidad emplean técnicas avanzadas, como las pruebas de conocimiento cero (ZKP), las firmas en anillo y las transacciones confidenciales, lo que permitiría realizar transacciones médicas sin exponer información sensible. Esto asegura que solo las partes autorizadas puedan identificar o verificar los datos sin comprometer la privacidad de los involucrados.
2. Protección contra la trazabilidad: Mediante métodos como las firmas en anillo (utilizadas en monedas como Monero), las monedas de privacidad impiden la correlación entre los datos del paciente y su historial clínico. Esto garantiza que las direcciones públicas de las transacciones no puedan asociarse a una identidad o historial específico, protegiendo aún más la privacidad de los pacientes.
3. Cumplimiento regulatorio y control del acceso: Estas monedas permiten almacenar datos sensibles de forma pseudonimizada o anonimizada, alineándose con los principios de privacidad por diseño. Además, ofrecen mecanismos como los *tokens* de acceso temporales, los cuales permiten a los pacientes otorgar y revocar permisos sobre sus datos. Así, el paciente mantiene un control soberano sobre su información de salud, decidiendo quién puede acceder a ella y bajo qué condiciones.
4. Eliminación de intermediarios en transacciones descentralizadas: Las monedas de privacidad facilitan transacciones sin la necesidad de intermediarios para manejar datos médicos sensibles. Este enfoque descentralizado contribuye a reducir riesgos asociados con actores externos y a aumentar la eficiencia del sistema.
5. Flexibilidad y escalabilidad en entornos eHealth: Monedas como Zcash utilizan técnicas como zk-SNARKs para validar transacciones de manera eficiente y confidencial, incluso en redes grandes. Este enfoque es ideal para sistemas de salud donde diversos actores (hospitales, aseguradoras, investigadores) deben procesar transacciones sin comprometer la privacidad de los datos.
6. Transparencia sin comprometer la privacidad: Aunque las monedas de privacidad aseguran la confidencialidad de los datos, también permiten verificar la integridad y autenticidad de los datos médicos sin revelar su contenido real. Esto permite mantener la transparencia dentro del sistema sanitario, alineándose con los principios de seguridad y privacidad.

3.3. ¿Qué trabajos abordaron temas relacionados con el problema central?

Existen varias propuestas que buscan simplificar la gestión de registros médicos en el sector de la salud mediante la combinación de tecnologías innovadoras y arquitecturas, otorgando a los pacientes control sobre sus datos médicos y garantizando su privacidad. Aunque estas soluciones no abordan directamente el uso de monedas de privacidad en historias clínicas electrónicas, muchas de ellas abordan aspectos claves de la seguridad, privacidad e interoperabilidad en sistemas descentralizados de salud, donde la integración de monedas de privacidad podría añadir una capa adicional de protección.

Un ejemplo es el modelo arquitectónico *multilayer* propuesto por Majumder et al. (2021) que combina una *blockchain* de consorcio (Ethereum), un servidor FHIR (Fast Healthcare Interoperability Resources; para asegurar un formato común y compartible de datos) y aplicaciones auxiliares para gestionar accesibilidad, autenticación, autorización y auditoría de registros médicos. Este sistema permite compartir datos de manera controlada y segura entre pacientes, médicos autorizados y personal clínico, manteniendo al paciente anónimo o pseudónimo según el caso. La integración de monedas de privacidad podría reforzar aún más la protección de los datos, garantizando una mayor confidencialidad en las transacciones. Además, propone la integración de Hyperledger Fabric para la gestión de datos y transacciones, e Hyperledger Explorer para la visualización de las transacciones, lo que facilita la interoperabilidad y la confianza entre los actores.

En una línea similar, Rincón y Moreno-Sandoval (2021) proponen una solución basada en Hyperledger Fabric que aprovecha sus características de inmutabilidad, algoritmos de consenso y contratos inteligentes (*smart contracts*) para asegurar el transporte seguro de información sensible. Aquí, la implementación de monedas de privacidad como Monero o Zcash podría integrarse para proteger la identidad y asegurar la confidencialidad de los datos durante las transacciones.

La integración de *blockchain* con tecnologías relacionadas con la Internet de las cosas médicas (IoMT) también ha sido explorada. Dalal et al. (2023) proponen un conector FHIR for Azure que asegura una conexión fluida entre dispositivos IoMT mediante redes P2P de *blockchain* e interoperabilidad con el estándar FHIR, utilizando criptografía asimétrica, firmas digitales y encriptación de *hash* para garantizar la privacidad de los datos y el control de acceso. Otra propuesta relacionada a la tecnología IoMT es la de Duvey et al. (2024), quienes proponen un proceso de aseguramiento de datos en la nube, donde los datos sensibles se cifran utilizando el esquema ECIES (*Elliptic Curve Integrated Encryption Scheme*) y se almacenan en múltiples nubes para mayor seguridad. La integración de monedas de privacidad en arquitecturas de IoMT podría añadir una capa crucial de anonimato y protección en el intercambio de datos sensibles entre dispositivos y actores de la nube. Combinando estas tecnologías, se lograría un nivel superior de seguridad, evitando la correlación de las transacciones con identidades reales. Sin embargo, como señalan Gadala et al. (2022), es fundamental abordar la complejidad de este desafío, considerando las diversas perspectivas involucradas y utilizando métodos estructurados que equilibren adecuadamente los compromisos entre seguridad y usabilidad. Esta combinación permitiría asegurar que, además de proteger la confidencialidad de los datos, se mantenga la funcionalidad y accesibilidad de los sistemas para los actores autorizados en los entornos de salud conectados.

En cuanto a la mejora de la interoperabilidad, Carter et al. (2019) sugieren la integración de Amazon Web Services (AWS) con *blockchain* Ethereum para facilitar el intercambio seguro de datos médicos, ofreciendo mayor seguridad y eficiencia en la gestión de información. El uso de monedas de privacidad en esta arquitectura podría asegurar que el intercambio de datos no revele detalles sensibles durante la transmisión o almacenamiento, agregando un nivel extra de confidencialidad.

En Rahman et al. (2019) se propone una arquitectura basada en una capa de abstracción llamada "blockchain handshaker", que permite integrar las capacidades de una *blockchain* pública sin necesidad de construir soluciones desde cero, lo que reduce costos y complejidad y mantiene la independencia entre la lógica empresarial y las tecnologías de *blockchain*. Las monedas de privacidad podrían ser una adición valiosa en este contexto, asegurando que la información de los pacientes permanezca privada incluso mientras se aprovechan las capacidades de la *blockchain* pública.

En el ámbito de la seguridad y privacidad, Vyas et al. (2020) y Nabil et al. (2022) exploran el uso de contratos inteligentes de Ethereum como una extensión útil para mantener los registros de salud seguros. Estas soluciones podrían beneficiarse de la integración con tecnologías de privacidad, como las monedas de privacidad, que añadirían un nivel adicional de protección, asegurando que los datos y transacciones sean invisibles incluso a las partes autorizadas si no se requiere su acceso.

En una línea similar, Yang et al. (2023) proponen la combinación de contratos inteligentes con el estándar HL7 FHIR[5] y *tokens* no fungibles (NFTs) para mejorar la gestión de los registros médicos electrónicos, mientras que Rao y Mat Kiah (2023) añaden técnicas de Apache Kafka para superar las limitaciones de escalabilidad de Ethereum. Las monedas de privacidad, al integrarse en estas soluciones, podrían garantizar la protección de los datos en todo el proceso, desde su recopilación hasta su uso final.

Otro desarrollo es el planteado por Wu et al. (2019) con un prototipo basado en React-Health-Documents que utiliza *blockchain* para rastrear documentos de salud de pacientes, almacenando *hashes* de los registros en Bitcoin para garantizar su permanencia. El uso de monedas de privacidad podría proteger aún más los datos, asegurando que solo los actores autorizados puedan ver los detalles completos de los registros.

Una propuesta del uso los mecanismos de privacidad como *zero-knowledge proofs* (ZKPs) utilizados por las monedas de privacidad es la de Saroop (2024), que analiza cómo los ZKP permiten validar información sin revelar datos sensibles.

Finalmente, algunos de estos modelos, junto con aquellos que podrían incorporar monedas de privacidad, se pueden probar en el GPOC Sandbox, una herramienta técnica diseñada para investigar y probar conceptos enfocados en la seguridad, cifrado homomórfico, descentralización, gestión de archivos y control de acceso. Según Davids et al. (2024) la moneda de privacidad más adecuada para implementar en GPOC Sandbox es Zcash, que utiliza el mecanismo de privacidad zk-SNARKs (pruebas de conocimiento cero). También se menciona Mina Protocol, que, aunque no es una moneda de privacidad en el sentido tradicional, tiene características que lo hacen adecuado para proteger datos sensibles en escenarios similares.

En la tabla siguiente se resumen los principales aportes para cada pregunta de investigación:

5 Fast Healthcare Interoperability Resources: estándar desarrollado por Health Level Seven International (HL7) para el intercambio de datos en salud. FHIR combina los principios de interoperabilidad con tecnologías web modernas, permitiendo una integración flexible y eficiente entre sistemas de información médica.

Tabla 5. Principal aporte de cada artículo

Preguntas de investigación	Aportes relevantes
P1: ¿ Qué modelos o propuestas de implementación de monedas de privacidad en historias clínicas han sido documentados en la literatura académica?	Pareek et al. (2024) Lee y Song (2021)
P2: ¿Qué ventajas ofrecen las monedas de privacidad como mecanismos de protección de datos en el ámbito de la salud?	Saroop (2024) Bernal Bernabe et al. (2019)
P3: ¿Qué trabajos abordaron temas relacionados con el problema central?	Duvey et al. (2024), Gadala et al. (2022), Ghesmati et al. (2022), Munilla Garrido et al. (2022), Wairimu y Fritsch (2022), Rahman et al. (2019), Wairimu y Fritsch (2022), Vyas et al. (2020), Yang et al. (2023), Rao y Mat Kiah (2023), Majumder et al. (2021), Nabil et al. (2022), Hoang et al. (2021), Rincón y Moreno-Sandoval (2021), Dalal et al. (2023), Mchale et al. (2023), Saroop (2024)

3.4. Consideraciones legales y normativas

La implementación de tecnologías emergentes como *blockchain* y monedas de privacidad en el ámbito sanitario no puede desvincularse del marco legal y normativo vigente, especialmente en lo que respecta a la protección de los datos personales de salud, considerados como información sensible por numerosas legislaciones. Si bien el presente estudio se focaliza en los aspectos técnicos y de privacidad desde una perspectiva computacional, resulta imprescindible incluir una reflexión crítica sobre las implicancias legales y regulatorias que condicionan su viabilidad y aplicación.

Protección de datos personales en salud

El tratamiento de historias clínicas electrónicas en Argentina se encuentra regulado por la Ley 25326 de Protección de los Datos Personales (del año 2000), que define a los datos de salud como datos sensibles y establece principios y garantías para su recolección, procesamiento y almacenamiento; por la Ley 26529 de Derechos del Paciente (del año 2009), que reconoce la historia clínica como un documento privado y garantiza el derecho de acceso del paciente a su contenido, así como a recibir información clara y comprensible sobre diagnósticos y tratamientos; y por la Ley 27706 (del año 2023), que crea el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas con el objetivo de implementar el Sistema Único de Registro de Historias Clínicas Electrónicas a nivel nacional, integrando los principios de estandarización, interoperabilidad, confidencialidad y seguridad de los datos personales en el ámbito de la salud.

A nivel internacional, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea,

2016) también impone obligaciones estrictas respecto al consentimiento explícito, el derecho al acceso, la rectificación y supresión de los datos, así como el principio de privacidad desde el diseño y por defecto, todos aspectos críticos que deben considerarse al utilizar tecnologías inmutables como *blockchain*.

Estándares técnicos y normativas internacionales

La gestión segura de la información médica digital puede apoyarse además en normas técnicas internacionales como la ISO/IEC 27799:2016 (actualización en desarrollo), que proporciona directrices específicas para la protección de información de salud personal en los sistemas de información. En términos de interoperabilidad, estándares como HL7 y FHIR (hl7.org, s.f.) definen marcos estructurados para el intercambio de datos clínicos entre sistemas heterogéneos, siendo fundamentales para garantizar la compatibilidad y legalidad de las soluciones tecnológicas propuestas.

Desafíos legales del uso de monedas de privacidad

Si bien las *privacy coins* como Monero o Zcash aportan mecanismos criptográficos robustos para garantizar el anonimato y la protección de datos, su nivel de ofuscación puede generar tensiones legales. La imposibilidad de rastrear ciertas transacciones podría entrar en conflicto con requerimientos legales que exigen trazabilidad en contextos como auditorías, litigios judiciales o investigaciones regulatorias. En consecuencia, se plantea la necesidad de definir modelos híbridos que permitan auditoría controlada bajo condiciones legalmente justificadas, sin comprometer la privacidad del paciente en escenarios ordinarios.

Implicancias éticas y necesidad de regulación específica

La incorporación de monedas de privacidad en la gestión de historias clínicas también plantea desafíos éticos vinculados al consentimiento informado, la transparencia y la rendición de cuentas.

4. Conclusiones

El análisis de la aplicación de las monedas de privacidad en el ámbito de la salud, especialmente en lo que respecta a la gestión de historias clínicas electrónicas, revela importantes desafíos en la protección de datos sensibles.

1. **Modelos de implementación de monedas de privacidad en el sector salud**: Aunque no se han encontrado implementaciones que utilicen monedas de privacidad directamente en una historia clínica electrónica, sí existen enfoques innovadores en la literatura que exploran la aplicación de tecnologías descentralizadas y *privacy coins* para mejorar la privacidad y la seguridad de los datos médicos. Ejemplos como los modelos propuestos evidencian cómo las monedas de privacidad pueden complementar sistemas de *blockchain* para la protección de datos médicos, mediante la adopción de mecanismos como las firmas en anillo y las pruebas de conocimiento cero.

2. **Ventajas de las monedas de privacidad en la protección de datos en salud**: Puede concluirse que las monedas de privacidad, como Monero y Zcash, ofrecen ventajas significativas en la protección de los datos de salud, destacándose por su capacidad de anonimización robusta, protección contra la trazabilidad y control granular del acceso a la información. Estas propiedades permiten que los pacientes mantengan el control soberano sobre sus datos, pudiendo otorgar o revocar permisos de acceso según sus necesidades. Sin embargo, en ciertos escenarios, como en procedimientos legales, es fundamental equilibrar privacidad y trazabilidad. Debido al anonimato inherente de la criptomoneda, es posible romper el vínculo entre la dirección sigilosa de un usuario autenticado y sus datos biométricos, preservando su identidad sin comprometer la integridad de los registros. Para garantizar este equilibrio, se pueden definir nociones de privacidad e identidad que operen independientemente de la moneda de privacidad subyacente, permitiendo mecanismos de auditoría controlada sin exponer innecesariamente la información personal. De esta manera, la seguridad del modelo puede asegurarse dentro de un marco flexible que proteja la privacidad del paciente, pero que a su vez posibilite la trazabilidad en situaciones justificadas, como procesos judiciales o auditorías regulatorias.

3. **Trabajos relacionados con la protección de datos médicos**: Se exploran soluciones tecnológicas que mejoran la interoperabilidad y la seguridad de los datos médicos, como las implementaciones de *blockchain* combinadas con FHIR, IoMT y contratos inteligentes. Estos trabajos presentan una base sólida sobre la que se pueden integrar monedas de privacidad para reforzar aún más la protección de la identidad y la confidencialidad de los datos. La integración de monedas de privacidad en estos modelos podría añadir una capa adicional de seguridad al garantizar que las transacciones de datos sensibles no sean correlacionables con identidades reales. Sin embargo, la implementación de estas soluciones debe abordar la complejidad del problema desde múltiples perspectivas, equilibrando adecuadamente la seguridad con la usabilidad para garantizar que los sistemas sean tanto seguros como prácticos para su adopción en entornos de salud reales.

En resumen, aunque la literatura no muestra implementaciones directas de monedas de privacidad en las historias clínicas electrónicas, se vislumbra un potencial considerable para su integración en sistemas de salud basados en *blockchain*, con el objetivo de mejorar la seguridad, privacidad y control sobre los datos médicos. La combinación de tecnologías emergentes, como la *blockchain*, IoMT y las monedas de privacidad, ofrece una solución robusta para los desafíos de privacidad y protección de datos en el ámbito de la salud; pero requiere una consideración cuidadosa de los compromisos entre seguridad y usabilidad.

Aunque este estudio se centró exclusivamente en monedas de privacidad, se reconoce como una limitación que este enfoque pudo haber excluido trabajos relevantes que emplean tecnologías *blockchain* más generales. En consecuencia, en otro estadio se propone ampliar la cadena de búsqueda incluyendo términos a fin de identificar otras implementaciones actuales que, aunque no utilicen monedas de privacidad de forma explícita, integren arquitecturas compatibles o mecanismos criptográficos aplicables a la protección de datos sensibles en historias clínicas electrónicas.

Si bien el mapeo sistemático se basó en el concepto de privacy coins, se reconoce que el término "monedas" suele asociarse principalmente al ámbito financiero, lo que podría generar confusión en el contexto de la salud. Por esta razón, se busca un término más adecuado que conserve la esencia de privacidad y control descentralizado sin la connotación económica. En este sentido, se propone a futuro el uso de *health privacy tokens*, una denominación que resalta su función como credenciales seguras y cifradas para la gestión de información médica, permitiendo a los pacientes controlar el acceso a sus datos de manera segura y privada dentro de una infraestructura basada en *blockchain*.

Referencias

Akcora, C. G., Gel, Y. R., y Kantarcioglu, M. (2022). Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota. En *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(1). John Wiley and Sons Inc. https://doi.org/10.1002/widm.1436

Ballandies, M. C., Dapp, M. M., y Pournaras, E. (2022). Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation. *Cluster Computing*, *25*(3), 1817-1838. https://doi.org/10.1007/s10586-021-03256-w

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., y Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. En *IEEE Access, 7*, 164908-164940. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2950872

Carter, G., Shahriar, H., y Sneha, S. (2019). Blockchain-based interoperable electronic health record sharing framework. *Proceedings - International Computer Software and Applications Conference*, *2*, 452-457. https://doi.org/10.1109/COMPSAC.2019.10248

Dalal, S., Lilhore, U. K., Simaiya, S., Sharma, A., Jaglan, V., Kumar, M., Jangra, M., Goyal, N., y Rana, A. K. (2023). A Blockchain-based secure Internet of Medical Things framework for smart healthcare. *Journal of Autonomous Intelligence*, *6*(3). https://doi.org/10.24294/jai.v6i3.592

Davids, J., ElSharkawy, M., Ashrafian, H., Herlenius, E., y Lidströmer, N. (2024). *Technical Sandbox for a Global Patient co-Owned Cloud (GPOC)*. https://doi.org/10.21203/rs.3.rs-3004979/v2

Duvey, A. A., Rahi, P., Ganesh, N. S. G., y Basa, S. S. (2024). Smart framework for enhancing security of IoT linked devices in Healthcare Systems. *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*. https://doi.org/10.1145/3647444.3647902

Gadala, M., Strigini, L., y Fujdiak, R. (2022, 23 de agosto). Authentication for Operators of Critical Medical Devices: A Contribution to Analysis of Design Trade-offs. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3544474

Ghesmati, S., Fdhila, W., y Weippl, E. (2022). SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Privacy Techniques. *Proceedings of the 17th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3538969.3538971

hl7.org. (s.f.). *FHIR - HL7*.

Hoang, H. Do, Hien, D. T. T., Nhut, T. C., Quyen, P. D. T., Duy, P. T., y Pham, V. H. (2021). A Blockchain-based Secured and Privacy-Preserved Personal Healthcare Record Exchange System. *Proceedings of the 2021 IEEE International Conference on Machine Learning and Applied Network Technologies, ICMLANT 2021*. https://doi.org/10.1109/ICMLANT53170.2021.9690542

Kitchenham, B., y Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, *55*(12), 2049-2075. https://doi.org/10.1016/j.infsof.2013.07.010

Kumar Dubey, P., Singh, B., Singh, D., y Singh, M. K. (2024). Blockchain for health care: A review. In A. J. Obaid, V. Kumar Shukla, S. Dutta, A. Bhattacharya, y S. Chakraborti (Eds.), *Blockchain Technology for Healthcare Applications: Challenges, Privacy, and Securing of Data* (pp. 50-75). Nova Science Publishers, Inc. https://doi.org/10.52305/AUFT8731

Lee, D., y Song, M. (2021). MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address. *IEEE Access*, *9*, 158122-158139. https://doi.org/10.1109/ACCESS.2021.3130552

Ley 25326. (2000). Protección de Datos Personales. https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

Ley 26529. (2009). Derechos del paciente en su relación con los profesionales e instituciones de la salud. 21 de Octubre de 2009. https://www.argentina.gob.ar/normativa/nacional/ley-25629-77155/texto

Ley 27706. (2023). Creación del Programa federal único de informatización y digitalización de historias clínicas de la República Argentina. 16 de Marzo de 2023. https://www.argentina.gob.ar/normativa/nacional/ley-27706-380710/texto

Majumder, A., Saha, S., Bhowmik, T., y Basu, A. (2021). A Conceptual Framework for Blockchain-based Intelligent Healthcare Data Management. 2021 *IEEE Bombay Section Signature Conference, IBSSC 2021*. https://doi.org/10.1109/IBSSC53889.2021.9673339

Mchale, S., Murr, L., y Zhang, P. (2023). *Using Decentralized Identifiers and InterPlanetary File System to Create a Recoverable Rare Disease Patient Identity Framework*, 142-149. https://doi.org/10.1145/3608298.3608325

Munilla Garrido, G., Sedlmeir, J., y Babel, M. (2022). Towards Verifiable Differentially-Private Polling. *Proceedings of the 17th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3538969.3538992

Nabil, S. S., Alam Pran, M. S., Al Haque, A. A., Chakraborty, N. R., Chowdhury, M. J. M., y Ferdous, M. S. (2022). Blockchain-based COVID vaccination registration and monitoring. *Blockchain: Research and Applications*, *3*(4). https://doi.org/10.1016/j.bcra.2022.100092

Pareek, V., Saran, D., Sharma, L., Jakhar, P., y Kumar, S. (2024). Blockchain Technology in Pharmaceutical Industry: A Review of Recent Research Articles on PubMed. *Scripta Medica (Banja Luka)*, *55*(3), 357-369. https://doi.org/10.5937/scriptamed55-47100

Parlamento Europeo, y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo Europeo. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

Rahman, M. S., Khalil, I., Mahawaga, P. C., Bouras, A., y Yi, X. (2019). A novel architecture for tamper proof electronic health record management system using blockchain wrap-

per. *BSCI 2019 - Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-Located with AsiaCCS 2019*, 97-105. https://doi.org/10.1145/3327960.3332392

Rao, I. S., y Mat Kiah, M. L. (2023). Innovative Framework for Secure Healthcare Data Management: Utilizing Ethereum Blockchain. *ETELEMED 2023: The Fifteenth International Conference on EHealth, Telemedicine, and Social Medicine*,16-22.

Rincón, E. A. P., y Moreno-Sandoval, L. G. (2021). Design of an architecture contributing to the protection and privacy of the data associated with the electronic health record. *Information (Switzerland)*, *12*(8). https://doi.org/10.3390/info12080313

Saroop, S. (2024). Blockchain-Based Zero-Knowledge Proofs for Data Privacy: Explore the Application of Blockchain Technology in facilitating Privacy-Preserving Transactions through Zero-Knowledge Proofs and Analyze their Effectiveness in Protecting Sensitive Data. *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*. https://doi.org/10.1145/3647444.3652463

SeguriLatam. (2022, 15 de marzo). *Ciberseguridad en el sector Salud: principales riesgos*. https:/www.segurilatam.com/actualidad/ciberseguridad-en-el-sector-salud-principales-riesgos_20220315.html

Shrivastava, S., y Srikanth, T. K. (2022). A Framework for Secure and Privacy Preserving Health Data Exchange across Health Information Systems using a Digital Identity System. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 41-49. https://doi.org/10.1145/3560107.3560115

Todo Noticias (TN). (2024, 19 de octubre). *Mes de la ciberseguridad: la alarmante situación de los sistemas de salud en la Argentina*. TN Tecno. https://tn.com.ar/tecno/novedades/2024/10/19/mes-de-la-ciberseguridad-la-alarmante-situacion-de-los-sistemas-de-salud-en-la-argentina/#:~:text=Los%20ciberataques%20se%20multiplican%3A%204%20de%20cada%2010,en%20aumento%2C%20los%20ciberataques%20pueden%20tener%20consecuencias%20devastadoras.

Vyas, J. D., Han, M., Li, L., Pouriyeh, S., y He, J. S. (2020). Integrating blockchain technology into healthcare. *ACMSE 2020 - Proceedings of the 2020 ACM Southeast Conference*, 197-203. https://doi.org/10.1145/3374135.3385280

Wairimu, S., y Fritsch, L. (2022, 23 de agosto). Modelling privacy harms of compromised personal medical data - Beyond data breach. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3544462

Wu, H., Shang, Y., Wang, L., Shi, L., Jiang, K., y Dong, J. (2019). A patient-centric interoperable framework for health information exchange via blockchain. *ACM International Conference Proceeding Series*, 76-80. https://doi.org/10.1145/3376044.3376055

Yang, C.-N., Kuo, H.-C., y Cheng, H.-H. (2023). Ensuring FHIR Authentication and Data Integrity by Smart Contract and Blockchain Enabled NFT. *ICMHI 2023*, 123-128. https://doi.org/10.1145/3608298.3608322

Guillermina Rosana Nievas
Perfil académico y profesional: Magister en Administración de Negocios y en Ingeniería de Software y Sistemas de Información. Especialista en docencia universitaria. Ingeniera en Sistemas de Información. Doctoranda en Informática en la Universidad Abierta Interamericana (UAI). Decana de la Facultad de Ingeniería de la Universidad Católica de Salta (UCASAL). Fue secretaria académica, jefa de carrera y jefa del Departamento de Extensión en la misma facultad. Docente universitaria de grado y posgrado desde 2000, en materias relacionadas con la auditoría de sistemas y la seguridad informática en la UCASAL y en la Universidad FASTA. En el ámbito profesional, se desempeña como consultora informática independiente con especialidad en el área de la salud y medicina, temática en la que también participa de proyectos de investigación.

Correo electrónico: gnievas@ucasal.edu.ar

Mario Matías Urbieta
Perfil académico y profesional: Doctor en Ciencias Informáticas por la Universidad Nacional de La Plata (UNLP), investigador y docente especializado en ingeniería de requerimientos, desarrollo de software dirigido por modelos e ingeniería web. Con una trayectoria de más de 15 años en el Laboratorio de Investigación y Formación en Informática Avanzada (LIFIA - UNLP/CIC), ha dirigido y codirigido proyectos de I+D vinculados a inteligencia artificial, aplicaciones web adaptables, ciencia ciudadana y procesamiento de datos satelitales. Ha formado recursos humanos en grado y posgrado en la Universidad Nacional de La Plata, la Universidad Católica de Santiago del Estero y la Universidad Abierta Interamericana. Ha evaluado proyectos y publicaciones científicas, y cuenta con producción académica en revistas y congresos internacionales.

Correo electrónico: murbieta@lifia.info.unlp.edu.ar