BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
NOTAS TÉCNICAS E INFORMES BREVES

Mi Data Share holístico: Una aplicación WEB3 para compartir datos: Más allá de las finanzas, un intercambio descentralizado y protegido de datos multidimensionales para mejorar la atención sanitaria mundial.

Sathya Krishnasamy, MS

ChainAim, Newington, Connecticut, EE.UU. DOI:

https://doi.org/10.30953/bhty.v7.341

Autor correspondiente: Sathya Krishnasamy, Correo electrónico: sathya.krishnasamy@chainaim.com

Palabras clave: control de acceso, blockchain, libro mayor distribuido, sanidad, privacidad, criptografía de umbral

Resumen

Las tecnologías WEB3 sobre arquitecturas de red, libros de contabilidad distribuidos e inteligencia artificial descentralizada representan un cambio transformador en la forma de manejar, almacenar y compartir los datos. Estas innovaciones prometen mejorar significativamente los derechos de privacidad de los datos de los consumidores al abordar vulnerabilidades fundamentales asociadas a los sistemas cen-tralizados tradicionales y a los monederos de autocustodia. Las filtraciones de datos en los sistemas tradicionales gestionados principalmente por terceros son más frecuentes y dan lugar a importantes fugas de datos debido al almacenamiento centralizado y al excesivo movimiento de datos, a veces innecesario. Las filtraciones de datos sanitarios han sido una preocupación creciente en todo el mundo. Varios hospitales se han enfrentado a paradas operativas debido al impacto del ransomware en la atención y la privacidad de los pacientes. WEB3 Las carteras son un componente vital que emerge como una fuerza significativa para la inclusión financiera global, especialmente en las economías en desarrollo. Promueven la inclusión, reducen costes y empoderan a los individuos a través de la autocustodia. Aunque estos monederos necesitan importantes mejoras, su uso no deja de aumentar. Se espera que la base mundial de usuarios de criptodivisas supere los 500 millones en 2025, con un crecimiento sustancial en los mercados emergentes, según un informe de Statista de 2023. Este artículo introduce un concepto que va más allá de las criptomonedas y las finanzas y se centra en casos de uso cotidiano en el mundo real que requieren un acceso combinatorio a los datos holísticos de una persona, incluidos los registros financieros y sanitarios, los datos genómicos y las directivas avanzadas, entre otros, que deben protegerse y compartirse con actores específicos identificados por sus funciones en el ecosistema WEB3 mediante identificadores descentralizados e insignias de tokens no fungibles que identifican a destinatarios concretos. El autor presentó el concepto en ETHBoston en abril de 2024, recibió elogios por una implementación primitiva que utilizaba tecnologías de criptografía de umbral subyacentes, y lo mejoró en una aplicación conceptual holística de intercambio de datos para la atención sanitaria mundial, como se presenta en este documento.

Recibido: 1 de agosto de 2024; Aceptado: 25 de agosto de 2024; Publicado: 31 de agosto de 2024

WEB3 es un conjunto de tecnologías emergentes. Incluye los libros de contabilidad distribuidos, las identificaciones autosuficientes y la inteligencia artificial,
y promueve conceptos de propiedad de datos y activos. WEB3 ofrece una alternativa descentralizada a los sistemas bancarios tradicionales[1].Las tecnologías WEB3 facilitan el acceso a los servicios financieros a las poblaciones no bancarizadas o infrabancarizadas[2],reducen los costes de las transacciones y capacitan a los individuos para compartir datos de forma consumidora a través de carteras WEB3 de autocustodia. Además, los principios de intercambio de datos de la Web 3.0 se ajustan a las modernas leyes de privacidad de datos, mejorando el control del usuario sobre la información personal. Estas innovaciones prometen mejorar significativamente los derechos de privacidad de los datos de los consumidores abordando algunas vulnerabilidades fundamentales asociadas a los sistemas centralizados tradicionales.

Las violaciones de datos en los sistemas convencionales son más frecuentes y dan lugar a importantes fugas de datos debido a las vulnerabilidades del almacenamiento centralizado y al excesivo movimiento de datos, a veces innecesario. El potencial de las tecnologías WEB3 para mejorar los derechos de privacidad de los datos de los consumidores es un paso hacia un futuro más seguro. Las filtraciones de datos sanitarios son una preocupación creciente en todo el mundo. Varios hospitales se enfrentaron a paradas operativas a causa del ransomware, lo que repercutió en la atención y la privacidad de los pacientes[3].

Soberanía y control de los datos con la autocustodia En lo que respecta a los monederos WEB3, la autocustodia se refiere a la gestión de los activos digitales propios mediante la custodia de las claves privadas sin depender de terceros intermediarios, que podrían hacer un uso indebido de las c l a v e s . La autocustodia se ajusta fundamentalmente a los principios de privacidad de los datos, ya que hace hincapié en el control individual sobre los datos personales. Muchos artículos del reglamento general de protección de datos de la Unión definen los datos personales, la minimización de datos, la legalidad y los diseños de seguridad ante todo adecuados al riesgo y las notificaciones. Del mismo modo, las secciones de la Ley de Privacidad del Consumidor de Califor-nia abarcan disposiciones que definen la información personal, el derecho a saber, la exclusión voluntaria, la supresión y la no discriminación por disentimiento. Por lo que respecta a la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios, las normas clave son la privacidad (que garantiza que las entidades cubiertas y los socios comerciales protejan los datos de los consumidores), la seguridad (que impone salvaguardias administrativas, físicas y técnicas) y la notificación de cualquier infracción. Estas normativas estipulan que las personas tienen la propiedad de sus datos, deben dar su consentimiento explícito a los usuarios de sus datos y se recopila la información mini-necesaria para conservarla durante un periodo concreto para usos específicos, con plena audibilidad de las acciones de privilegio de acceso, uso y revocación de los datos. La autocustodia reduce la dependencia de terceros proveedores de servicios, reduciendo potencialmente el manejo indebido de datos o las infracciones cuyos sistemas no sean lo suficientemente seguros.

Limitaciones de los monederos actuales

Los monederos actuales almacenan activos cripto-nativos como criptomonedas y tokens no fungibles (NFTs) predominantemente para aplicaciones y servicios financieros y, hasta cierto punto, para almacenar coleccionables digitales. En estos casos de uso, los coleccionables se guardan en un almacenamiento descentralizado como el Sistema de Archivos Interplanetarios (IPFS) y tienen un puntero en el monedero y en los metadatos. Sin embargo, son posibles muchos casos de uso, ya que los mismos conceptos pueden aplicarse igualmente a la gestión del acceso a otras formas de información personal, además de los registros financieros. Entre ellos se incluyen los historiales médicos, los historiales genómicos, las directivas avanzadas, entre otros, en los que distintas formas de datos pueden necesitar ser vistas por personas que desempeñan papeles específicos en el contexto social, que son usos más lógicos.

La autocustodia requiere que las personas tengan conocimientos y experiencia en el manejo de sus claves privadas. Además, la experiencia de uso del monedero todavía no es muy sencilla y requiere cierta sofisticación técnica y seguir una serie de pasos no triviales. Algunos usuarios podrían necesitar asistencia técnica para gestionar sus claves y recurrir a terceros. Dependiendo de las capacidades de seguridad y la integridad de los custodios, esto puede conllevar riesgos, como el robo de identidad, la pérdida de fondos o la violación de la privacidad, entre otros.

Esto abre la necesidad de protocolos descentralizados que sean más resistentes que los custodios centralizados y de una descentralización a nivel de protocolo ciego a los datos que aumente la resistencia de la gestión de datos mediante el cifrado de la información de los usuarios y el uso de sistemas de gestión críticos descentralizados y gestionados por mecanismos criptográficos que puedan reensamblar las credenciales de acceso a los datos, basándose en funciones granulares para periodos específicos. Una tecnología clave que intenta lograr esta descentralización es la criptografía de umbral.

Criptografía de umbral

La criptografía de umbral es un esquema criptográfico en el que una clave criptográfica se divide en múltiples partes, distribuidas entre diferentes partes. Un número predefinido de estas partes (el umbral) debe combinarse para realizar operaciones criptográficas como el descifrado o la firma. Por ejemplo, si una clave se divide en 10 participaciones y el umbral se fija en 6, se pueden utilizar 6 participaciones cualesquiera para reconstruir la clave, pero menos de 6 participaciones no proporcionarán ninguna información sobre la clave. Cada acción estará en manos de un custodio concreto, que sólo conoce una parte de la clave, no toda.

Ventajas de la criptografía de umbral

Entre las ventajas de la criptografía de umbral se encuentran la mejora de la seguridad, la redundancia y la fiabilidad, y la autorización multipartita.

Mayor seguridad

Al distribuir claves compartidas entre varias partes, la criptografía de trillizos garantiza que ninguna entidad tenga acceso completo a la información sensible. Este enfoque mitiga el riesgo de acceso no autorizado y proporciona una capa adicional de seguridad para la gestión de registros críticos. En la práctica, esto significa que incluso si un actor malintencionado compromete una acción, no puede acceder a los datos sensibles ni realizar operaciones sin obtener el número mínimo requerido de acciones. Ningún individuo tiene el poder de comprometer los datos de forma independiente, lo que reduce drásticamente la probabilidad de que se produzcan filtraciones de datos y amenazas internas.

Redundancia y fiabilidad

La criptografía de umbral permite realizar operaciones aunque se pierdan o se pongan en peligro algunas claves compartidas, siempre que el número umbral de claves compartidas permanezca intacto. Esto garantiza que los registros críticos sigan siendo accesibles y seguros frente a problemas técnicos o fallos de seguridad.

Autorización multipartita

La criptografía de umbral ayuda a garantizar que los datos no puedan manipularse sin el consenso de varias partes. Esto facilita la colaboración segura al permitir a los investigadores compartir y analizar datos sin exponerlos en su totalidad a un único participante. Esto es especialmente

Citación: Blockchain en la sanidad hoy 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

Esto es especialmente importante en ensayos clínicos y estudios de investigación, donde la integridad de los datos es esencial para extraer conclusiones válidas y garantizar la seguridad de los pacientes. En situaciones en las que intervienen múltiples partes interesadas, como la planificación patrimonial o las voluntades anticipadas, la criptografía de umbral permite la autorización segura de múltiples partes. Esto garantiza que las decisiones o acciones relacionadas con registros sensibles requieran el consenso de múltiples partes autorizadas, lo que mejora la seguridad y la integridad.

Limitaciones y retos de la criptografía de umbral

La complejidad, la disponibilidad y la escalabilidad son limitaciones y retos.

Complejidad

La división de la clave criptográfica y la gestión de los recursos compartidos requieren protocolos sofisticados. Implementarlos correctamente y garantizar su resistencia ante diversos ataques a la seguridad es todo un reto.

Disponibilidad

Reconstruir la clave requiere la participación activa de varias partes, lo que puede resultar ineficaz si las partes están dispersas geográficamente o tienen una disponibilidad irregular.

Escalabilidad

A medida que aumenta el número de participantes y acciones, se incrementa la complejidad y la sobrecarga de comunicación y disponibilidad, lo que puede causar problemas de escalabilidad.

La implementación específica de la criptografía de umbral puede variar en función de cómo se difunda la distribución de claves criptográficas y cómo se configure el control de acceso para la recuperación de datos. El mecanismo de reensamblaje de las claves compartidas y el umbral también es configurable. En un modo de funcionamiento descentralizado, la implementación del protocolo puede descentralizar los fragmentos de claves entre los nodos validadores.

MyHolisticDataShare y las posibilidades de la sanidad mundial

MyHolisticDataShare es una aplicación WEB3 de compartición de datos que aborda las limitaciones e introduce nuevos con-ceptos de organización y almacenamiento de tipos de datos de usuario más allá de los datos financieros y los coleccionables digitales en activos del mundo real como los historiales médicos. Estas directivas avanzadas pueden gestionarse ampliando las primitivas criptográficas para compartir datos de forma segura. El acceso a estos registros se puede proporcionar y dosificar individualmente a partes específicas y a sus funciones en el contexto social, o podría ser una combinación de activos para un destinatario o una función en particular.

MyHolisticDataShare es una adaptación revisada y mejorada de la aplicación SocialSecureShare, concebida inicialmente por el autor en ETHBoston en abril de 2024, que ganó la votación al mejor proyecto de privacidad y comunidad. MyHolisticDataShare es un prototipo técnico para consumidores y receptores de dichos datos, que combina muchos aspectos del intercambio de datos dirigido por el consumidor y sus implicaciones para la atención sanitaria y los datos combinados con la salud en entornos habituales y de emergencia, y la salud y las finanzas para esfuerzos como los determinantes sociales de la atención.

Estas tecnologías emergentes de protección de la privacidad, como la criptografía de umbral y el control de acceso, muestran las posibilidades de promover el intercambio de datos a través del consumidor, al tiempo que permiten mejorar la privacidad reduciendo los puntos únicos de fallo, el control de acceso granular y componible, y la posibilidad de que entidades de control y equilibrio participen también como nodos para mejorar la visibilidad.

Diseño técnico de MyHolisiticDataShare MyHolisticDataShare utiliza primitivas de privacidad criptográficas y mecanismos descentralizados -como la criptografía de umbral para proteger la privacidad del acceso al descifrado de los datos encriptados almacenados de forma descentralizada- basados en NFT, que son fichas para identificar elementos únicos. Los NFT son fichas únicas que representan una cosa y sólo una cosa, y pueden utilizarse para representar una insignia específica. El gobierno del protocolo y la aplicación pueden asignar estas insignias.

MyHolisiticDataShare se basa en la aplicación descentralizada de la criptografía de umbral mediante el Protocolo de Umbral y el protocolo de Control de Acceso de Umbral (TACo)[4].Estos NFT se asignan a credenciales de identidad específicas asociadas a personas o funciones que proporcionan acceso a los datos del consumidor basándose en la verificación de identidad descentralizada de las carteras que poseen dichas credenciales de acceso.

La red umbral ofrece un conjunto completo de servicios descentralizados de criptografía umbral para aumentar la privacidad y soberanía del usuario en blockchains de permisos (Figura 1). La criptografía umbral protege los datos distribuyendo las operaciones a través de una red de nodos independientes, aumenta la seguridad y la disponibilidad y reduce la dependencia de las partes de confianza. La red Threshold utiliza el protocolo de servicio TACo para el control de acceso. El propietario de los datos puede cifrar su carga útil, que puede tener múltiples secciones, y puede almacenarlos en ubicaciones fuera de línea. En caso necesario, estos elementos de almacenamiento también pueden utilizarse en el almacenamiento descentralizado. En este ejemplo, el propietario de los datos almacena los datos cifrados en el IPFS, una popular solución de almacenamiento descentralizado.

El TACo divide un secreto conjunto -una clave de descifrado- en múltiples *partes* y las distribuye entre los operadores de nodos autorizados y con garantías (es decir, los interesados en la red umbral). Un número mínimo -un umbral- de los operadores que poseen las partes de la clave deben estar en línea y participar activamente en los descifrados parciales. Estos se combinan posteriormente en el cliente del solicitante para reconstruir los datos originales en texto plano. Cada carga de datos está sujeta a condiciones que pueden restringir el acceso de forma granular. El propietario de los datos puede definir una serie de condiciones de acceso que pueden incluir comprobaciones de control de acceso como, por ejemplo, "¿El

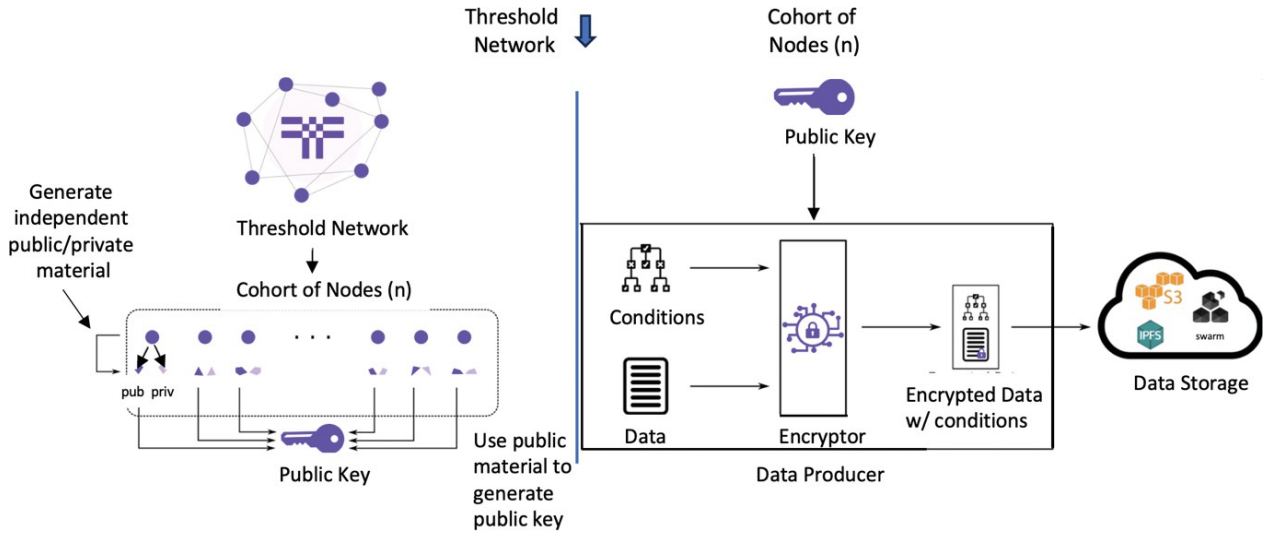

Fig. 1. Capturas de pantalla de la implementación de la criptografía umbral en la red. Fuente: https://docs.threshold.network/applications/threshold-access-control/key-concepts.
Fuente: Copyright del autor, 2024.

¿El solicitante posee una NFT específica que representa una insignia de un trabajador de emergencias médicas?" o "...un trabajador social que ayuda a los pacientes?". También puede combinarlos con otros elementos como: "¿El solicitante pide acceso durante un horario para el que el propietario de los datos da acceso, etc.?".

Los solicitantes demuestran su asociación con el cumplimiento de la condición -su derecho a recibir un número umbral de acciones de descifrado- mediante la firma de una transacción que verifica su propiedad de un determinado monedero WEB3 (en este caso, el monedero MetaMask en Polygon Test Network Amoy). Se comprueba que ese monedero cumple la condición específica (por ejemplo, poseer un NFT para poder acceder a los activos de datos).

MyHolisticDataShare está diseñado para estar compuesto por diferentes tipos de registros, como se ilustra en la Figura 2, que un consumidor podría almacenar en una infraestructura de almacenamiento descentralizada como el IPFS, con metadatos que definen el URI.

La implementación se realiza en Polygon blockchain Amoy Test Network, con el acceso de cartera MetaMask que almacena el control de acceso a través de insignias NFT.

Los usuarios pueden almacenar de forma flexible diferentes tipos de registros, incluyendo financieros, sanitarios, genómicos y directivas avanzadas.

Registros financieros

Estos podrían incluir cuentas financieras tradicionales, cuentas criptográficas, extractos bancarios, cartas de crédito, entre otros, que el usuario podría almacenar de forma segura y decidir compartir con destinatarios específicos que el usuario considere necesario compartir con fines específicos relacionados con las finanzas.

Registros sanitarios

Puede tratarse de historiales médicos básicos, incluidos informes de laboratorio, diagnósticos, imágenes de diagnóstico y citas que el usuario considere necesario compartir para fines sanitarios específicos.

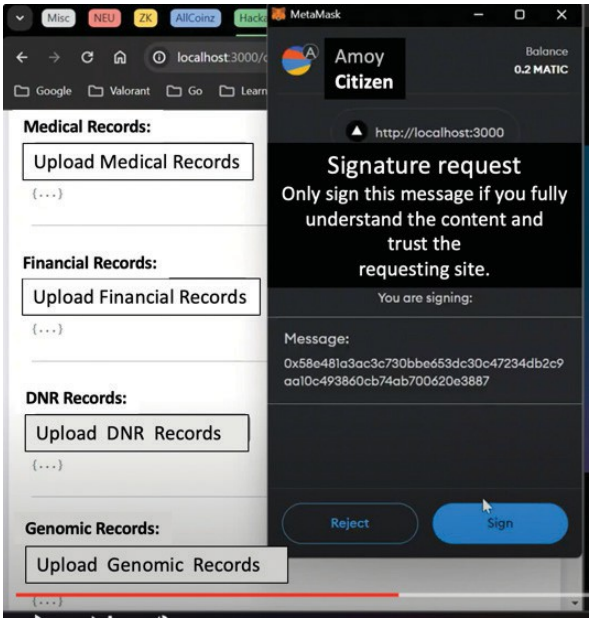

Fig. 2. Captura de pantalla de un registro de usuario encriptado. Fuente: Copyright del autor, 2024.

Registros genómicos

Podrían incluir información granular, altamente especializada y personal, como registros genómicos que el usuario puede compartir con investigadores y clínicos específicos de su interés.

Directivas avanzadas

Podrían incluir información específica de los poderes sanitarios sobre aspectos como las preferencias de "No Resucitar" (DNR), entre otros, que son importantes para el personal sanitario y los técnicos de emergencias.

Citación: Blockchain en la sanidad hoy 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

La figura 2 muestra una captura de pantalla del proceso en el que el propietario de los datos y un ciudadano en un entorno social firman la transacción al almacenar las diferentes cargas útiles de datos que desean cifrar para que se almacenen en un almacenamiento descentralizado. La Figura 3 muestra una captura de pantalla de la carga de datos y los detalles de la ubicación de almacenamiento descentralizado, y también muestra los mensajes de respuesta de acuse de recibo.

Insignias de destinatario de MyHolisticDataShare

Los participantes en la red Blockchain reciben distintivos NFT específicos administrados por una organización autónoma de datos que registra los identificadores descentralizados. Por ejemplo, a los identificadores descentralizados (DID) de la red se les puede asignar una insignia de médico de cabecera, y a otro DID se le puede asignar una insignia de técnico de emergencias médicas (EMT) que representa el contexto social específico de las necesidades de datos.

Los distintivos de contexto de datos sociales y sus configuraciones están disponibles en un registro que indica al usuario qué distintivos pueden acceder a qué tipo de datos. Por ejemplo, en la configuración por defecto, un paramédico puede tener acceso a los historiales médicos y a los registros de DNR, pero no a los registros financieros. Un investigador genómico podría poseer una insignia que muestre su interés por un tipo específico de datos genómicos que pudiera tener. El acceso combinado también podría controlarse granularmente. Por ejemplo, un trabajador social podría tener acceso a los historiales sanitarios y financieros para ayudar a planificar la ayuda a la coordinación de los determinantes sociales de la salud. La figura 4 muestra los distintos tipos de distintivos, almacenados como NFT que se guardarán en los monederos de los receptores de datos. Cuando el

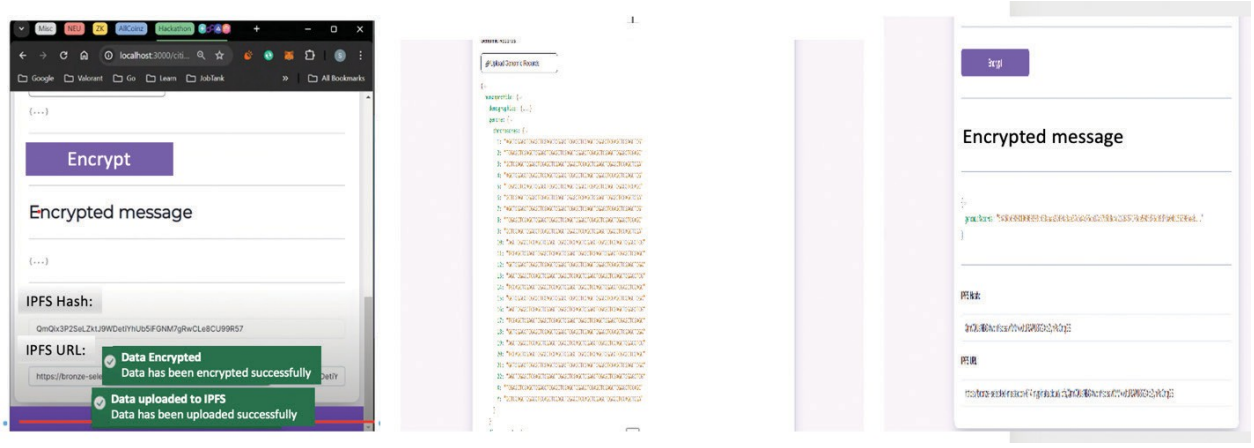

Fig. 3. Contenido cifrado con éxito basado en datos de muestra sintéticos. Fuente: Copyright del autor, 2024.

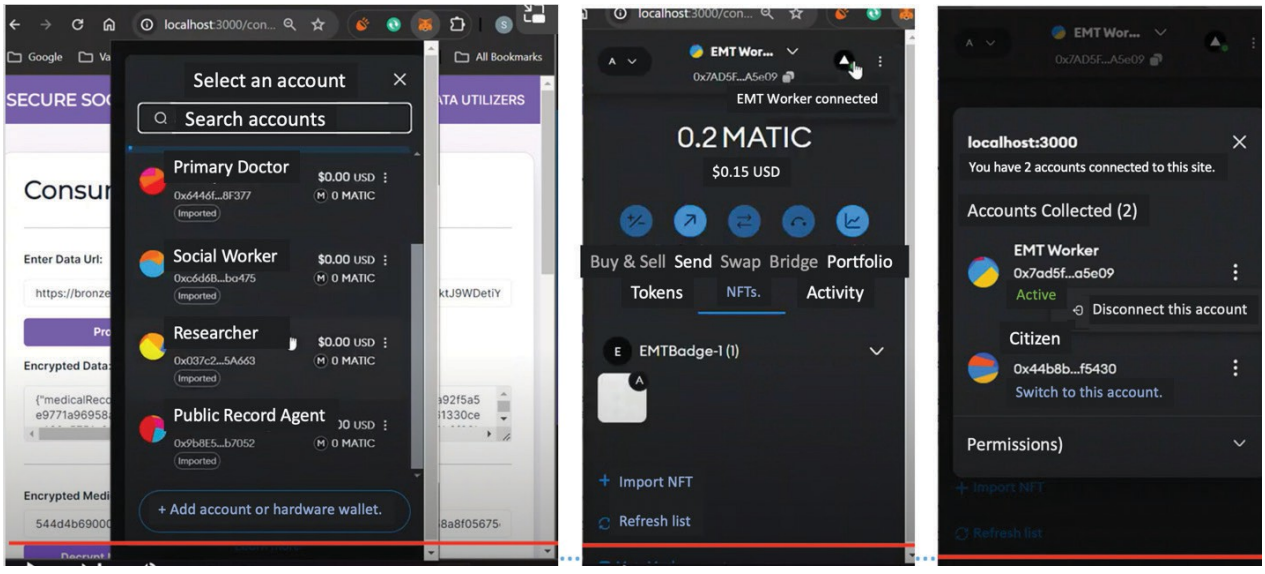

Fig. 4. Distintas insignias modeladas como NFT asignadas a identificaciones descentralizadas. EMT: técnico de emergencias médicas; ID: identificación; NFT: fichas no fungibles.
Fuente: Copyright del autor, 2024.

Cuando un destinatario de datos intenta acceder a los datos cifrados del propietario de los datos, en función de los controles de acceso definidos, se comprueba la presencia de estas fichas NFT para permitir o denegar el acceso.

Resultados del descifrado y disponibilidad de los datos

Basándose en las configuraciones de quórum de descentralización de la red y en las definiciones de NFT, el usuario puede firmar sus transacciones para encriptarlas de modo que estén disponibles para su desencriptación por DID específicos que tengan necesidades de datos específicas modeladas como definiciones de NFT únicas. Éstas también pueden modelarse, y el protocolo decen-tralizado comprobará un momento específico para el descifrado. El distintivo y las definiciones del protocolo darían acceso al descifrado. El acceso a cualquier otro dato no estará disponible. La figura 5 muestra la situación en la que se comprueba un distintivo NFT específico durante el descifrado, se verifica y ejecuta el derecho a descifrar y el descifrado se realiza con éxito. Los ejemplos incluyen el acceso legítimo a registros genómicos para un investigador designado o un trabajador sanitario de EMT con acceso a datos de DNR. La figura 6 muestra una situación en la que alguien que no disponga del distintivo NFT necesario no puede descifrar los datos. Por ejemplo, alguien que no disponga de un distintivo NFT de trabajador social no tiene acceso a los datos de los historiales médicos y financieros de los propietarios.

En el mundo real, la gobernanza que subyace a este protocolo y aplicación implicará la verificación fuera de línea para la emisión de los distintivos, posiblemente con la participación de una combinación de sistemas sanitarios y organizaciones sociales que definan las funciones y los criterios de acceso para la autorización del acceso. Por ejemplo, un trabajador social designado con controles de acceso específicos, que podría estar trabajando en funciones de coordinación de la atención o de atención comunitaria, puede acceder tanto al historial médico como al financiero para encontrar atención holística para ese paciente en función de su situación socioeconómica, donde la atención podría incluir algo más que atención médica, pero también encontrar vivienda, transporte y otras funciones que demuestren su necesidad.

A medida que maduran las cadenas de bloques sin permisos, observamos una tendencia creciente por parte de los consumidores a adoptar cadenas de bloques sin permisos, medida por carteras de autocustodia y participación en aplicaciones sociales basadas en WEB3 de diversas entidades e individuos. Estas actividades también pueden aprovecharse para la adopción de la privacidad de los datos sanitarios mediada por el consumidor si se planifican cuidadosamente con los controles y equilibrios adecuados, incluidos algunos nodos reguladores que se ejecuten en blockchains públicas/híbridas, algo que está empezando a suceder lentamente.

La criptografía de umbral no compite con otras técnicas de protección de la privacidad, sino que las complementa, como el cifrado totalmente homomórfico y la computación multipartita. En esos casos, los sistemas de umbral pueden añadir otra capa de seguridad, en la que el contenido encriptado puede ser de acceso controlado cuando el usuario no puede acceder a él.

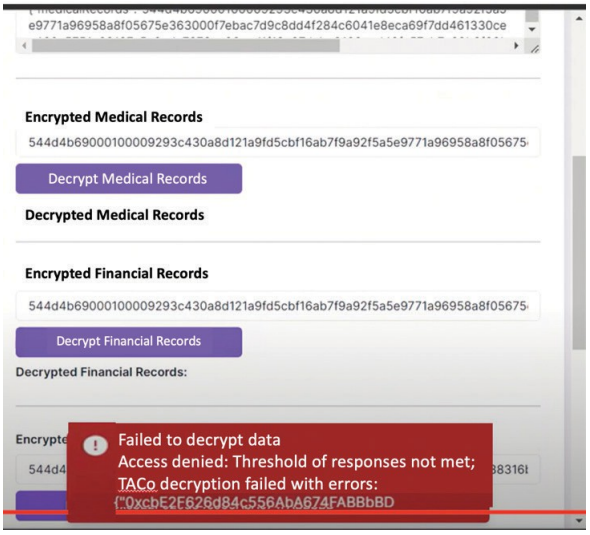

Fig. 6. Captura de pantalla de un acceso denegado basado en el control de acceso granular. TACo: Control de acceso por umbral. Fuente: Copyright del autor, 2024.

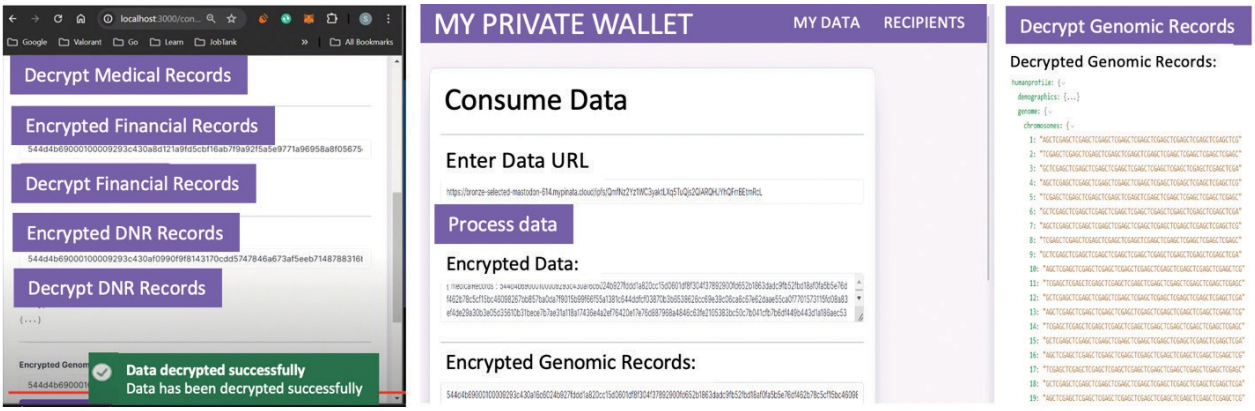

Fig. 5. Ejemplo de cifrado y descifrado de datos sintéticos de muestra con acceso legítimo. URL: localizador uniforme de recursos. Fuente: Copyright del autor, 2024.

Citación: Blockchain en la sanidad hoy 2024, 7: 341 - https://doi.org/10.30953/bhty.v7.341

El sistema solicitante accede a los datos desde puntos finales distribuidos o realiza cálculos sobre los datos cifrados. En esos contextos podría ser aún más crítico que los sistemas de control de acceso sean "a prueba de balas". En otro artículo contemporáneo, el autor habla de la aparición de las pruebas de conocimiento-cero y del aprendizaje automático, que también es muy complementario, y en el que se puede minimizar el intercambio de datos presentando pruebas para los verificadores. Este intercambio de datos holístico que preserva la privacidad también podría abordar otro problema, que son las violaciones de datos entre organizaciones y entre dominios. Por ejemplo, cuando se produce una filtración de datos en el sector minorista o bancario, puede verse comprometido el acceso a los historiales médicos, ya que se filtra información personal y se proporciona más información a los usuarios malintencionados. Sin embargo, con estos datos compartidos holísticos y un acceso granular y componible, los consumidores podrían tener más control sobre sus datos y estar en condiciones de responder mucho mejor a las adversidades.

Una de las principales mejoras que necesita WEB3 es la facilidad de uso para los consumidores, ya que para los usuarios es todo un reto seguir los pasos y las direcciones desconocidas. Este esfuerzo ya ha intentado mantener la UI/UX (diseño de interfaz de usuario/diseño de experiencia de usuario) muy cerca de una página web de Web 2, al menos en lo que respecta a la gestión de sus datos. Utiliza una conceptualización orientada a la usabilidad del consumidor en torno a estructuras de datos JSON (JavaScript Object Notation), estándares y pantallas sencillas. En las iteraciones posteriores, se intentará examinar cómo las definiciones de datos pueden estar también en una extensión del navegador y utilizar mecanismos avanzados de abstracción de cuentas y simplificación de iden-tidades para aumentar la usabilidad.

Conclusiones y trabajo futuro

MyHolisticDataShare ha demostrado una nueva extensión de las tecnologías WEB3 basada en la compartición descentralizada de datos y la criptografía de umbral para descentralizar el acceso de descifrado al quórum no centralizado y las definiciones de umbral configurables. Se trata aún de un concepto introductorio, y la versión final de la implementación dependerá de las definiciones del contexto normativo, del diseño de gobernanza de la Organización Autónoma Descentralizada, y de la madurez y el éxito de los procesos de gobernanza de DID en un contexto social.

Cualquier intento de probar las cadenas de bloques en entornos convencionales deberá planificarse cuidadosamente y dependerá de cadenas de bloques específicas, incluidas arquitecturas públicas/privadas/híbridas concretas. Este prototipo conceptual muestra formas alternativas en las que las tecnologías WEB3 abren soluciones potenciales para los problemas crónicos a los que se enfrentan los sistemas centralizados con la privacidad y el intercambio de datos, principalmente reduciendo los fallos de un único punto de confianza y el control de acceso granular y componible.

El autor tiene la intención de ampliar esta aplicación en una aplicación de monedero de extensión de navegador a medida que el panorama madure, específicamente en torno a cómo los monederos y las aplicaciones de intercambio de datos WEB3 y sus responsabilidades. Las tecnologías complementarias, como los sistemas de conocimiento cero y los cifrados totalmente homomórficos, pueden mejorar esta conceptualización para crear diseños mejorados y protegidos de la privacidad para el intercambio de datos iniciado y financiado por el consumidor. Los esfuerzos del autor en ChainAim continúan construyendo relaciones con organizaciones de normalización y fundaciones tecnológicas para identificar las necesidades de escalabilidad y las necesidades de gobernanza para avanzar en este intercambio de datos.

Financiación

Ninguna.

Conflictos de intereses

Ninguno.

Colaboradores

Sathya Krishnasamy es Presidente y Director de ChainAim Technologies. Sus 25 años de trayectoria abarcan una amplia experiencia en la gestión de sistemas de pago en importantes empresas sanitarias estadounidenses, como Aetna y Anthem. Se centra en las tecnologías emergentes, incluidos los sistemas de inteligencia artificial/aprendizaje automático y las tecnologías de libro mayor distribuido. También es asesor en muchas iniciativas del sector en materia de colaboración entre pagadores y proveedores, organizaciones de normalización e iniciativas como los agregadores de cuentas en la India, que promueven los sectores de la tecnología financiera, la sanidad y las competencias. Actualmente es presidente y director de ChainAim, que ofrece servicios de consultoría de estrategia técnica y desarrollo de aplicaciones.

Sathya Krishnasamy contribuyó a la investigación, conceptualización e implementación general.

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

No hay repositorios de datos.

Aplicación de texto generado por IA o tecnología relacionada

Ninguna.

Agradecimientos

Pankhuri Gupta, estudiante del Máster en Ingeniería de Software de la Universidad Northeastern de Boston (Massachusetts, EE.UU.), ayudó al director a diseñar y aplicar la interfaz de usuario. Se puede contactar con ella en gupta@pankh@ northeastern.edu.

Referencias

1. Buterin V. Ethereum whitepaper [Internet]. ethereum.org; 2014 [citado 2024 Ago 01]. Disponible en: https://ethereum.org/en/ whitepaper/
2. WEB3 and financial inclusion: bridging the gap [Internet]. www.linkedin.com. [citado 2024 ago 01]. Disponible en: https://

www.linkedin.com/pulse/WEB3- financial- inclusion- bridging-gap-liveplexplatform-ojazc/
3. Departamento de Salud y Servicios Humanos de los Estados Unidos [Internet]. HHS. gov.; 2019 [citado 2024 ago 01]. Disponible en: https://www.hhs.gov
4. Control de acceso de umbral (TACo). Threshold.network; 2024 [citado 2024 Ago 15]. Disponible en: https://docs.threshold.network/applications/threshold-access-control