



El panorama 2030 de identidad e interacciones digitales

Commercial White Paper

Resumen

Se prevé que en 2030 más del 30% de la población mundial utilizará billeteras digitales de identidad. Estas billeteras revolucionarán no solo la forma en que las personas controlan y utilizan sus identidades digitales, sino también la forma en que gestionan e intercambian valor. Como una extensión natural de las funcionalidades de las billeteras digitales de identidad, las billeteras digitales universales ofrecerán a las personas un canal integrado y seguro que combinará autenticación y pagos, agilizando numerosas interacciones del día a día, como el acceso a sitios web, la participación en programas de fidelización, el envío de dinero y el pago de bienes y servicios.

Mediante el uso de criptografía, las billeteras digitales de identidad ofrecerán una seguridad y un control por parte del usuario sin precedentes, dirigiéndonos hacia una web verificable y una economía digital global. A medida que evolucionan las tecnologías de IA y las computadoras cuánticas, los hackers de identidad contarán con herramientas extremadamente potentes y eficientes para el robo de contraseñas y la *impersonación* digital. En este escenario, las billeteras digitales universales surgen como la herramienta de salvaguarda, tomando la forma de aplicaciones móviles que ofrecen a los individuos la posibilidad de

manejar credenciales digitales de identidad protegida criptografía resistente tanto a la IA como a la computación cuántica.

Las billeteras de identidad no sólo impiden el robo de identidad, sino que también garantizan que cada interacción digital sea segura y esté autenticada dentro de los marcos de confianza establecidos. A medida que el mundo evoluciona hacia una economía digital global, la integridad y la fiabilidad de las interacciones digitales serán primordiales. Las billeteras digitales de identidad sientan una sólida base de seguridad, fomentando la confianza, la privacidad y la inclusión en el mundo digital.

La tecnología de Blerify está diseñada para acelerar la adopción de billeteras digitales tanto de identidad como universales. Nuestra plataforma integra tecnologías de vanguardia con principios de diseño centrados en el usuario. Asociarse con Blerify significa adoptar soluciones innovadoras que ofrecen seguridad, eficiencia e inclusión en las transacciones digitales de todo el mundo. Blerify invita a entidades de los sectores público y privado a sumarse a nuestra misión de ser pioneros en el futuro de las billeteras digitales y la gestión de identidades. Juntos, podemos impulsar la transformación que llevará a cada organización a prosperar en esta nueva era digital.



Índice

Resumen	2
1. Billeteras digitales universales	4
2. Billeteras digitales universales e Identidad Digital	7
3. Billeteras digitales universales y la Transferencia de Valor	14
4. El camino hacia las billeteras digitales universales	19
5. eWallets 2.0	24
6. Blerify habilita las billeteras digitales universales	29
Apéndice: Casos de uso por industria	45
Referencias	59

1. Billeteras Digitales Universales



Una billetera digital universal puede entenderse como un contenedor digital seguro que permite a las personas almacenar, gestionar e interactuar con diversos tipos de datos y activos. En la actualidad existen diferentes tipos de billeteras digitales, mayoritariamente de pagos. Sin embargo, las primeras billeteras de identidad están comenzando a surgir en el presente. Las billeteras universales, que combine manejo de identidad y pagos, llegarán inmediatamente después.

Una billetera digital universal permite gestionar tanto identidad como activos, posibilitando la interoperabilidad con instituciones públicas y privadas, así como con otros individuos. Sirve de canal unificado para que las personas gestionen todas las formas de interacción digital relacionadas con la verificación de datos y la transferencia de valor, ofreciendo las siguientes características:

- **Gestión de identidades:** Proporcionar almacenamiento y gestión seguros de credenciales de identidad personales o corporativas. Estas credenciales pueden incluir identificaciones electrónicas, contraseñas, claves privadas (por ejemplo, claves de acceso), tokens de autenticación y cualquier otro documento verificable. Esta función otorga a los usuarios un control total sobre sus datos de identidad, permitiéndoles gestionar, proteger y compartir su información de identidad de forma segura y eficiente a través de diversas plataformas y servicios.
- **Interacciones y transacciones:** Facilitar interacciones seguras con otros sistemas, redes o individuos. Esto incluye acceder a servicios, demostrar la identidad y participar en comunicaciones autenticadas. La billetera permite a los usuarios verificar su identidad, compartir credenciales verificables y participar en intercambios seguros de información a través de Internet.
- **Pagos:** Soportar la ejecución de pagos seguros entre partes, abarcando varias formas de transferencias financieras digitales, incluyendo moneda tradicional, tarjetas digitales de crédito y débito, y criptomonedas. Las funcionalidades de pago deben estar diseñadas para integrarse sin problemas con los sistemas financieros existentes de conformidad con la normativa para garantizar intercambios de valor fluidos, seguros y fiables tanto en entornos en línea como fuera de línea.
- **Gestión de activos:** Permitir a los usuarios almacenar y gestionar una amplia gama de activos digitales, como dinero electrónico, criptomonedas, certificados digitales y activos físicos representados en forma digital. Esta función proporciona a los usuarios una plataforma unificada para transferir valor.
- **Seguridad:** Incorporar sólidos mecanismos de seguridad, incluyendo encriptación, autenticación y control de acceso para proteger el contenido de la billetera de accesos no autorizados o robos. La arquitectura de seguridad de la billetera está diseñada para salvaguardar los datos y las transacciones de los usuarios con el fin de ofrecer el máximo nivel de protección.
- **Recuperabilidad:** Proporcionar mecanismos completos para recuperar el acceso al contenido de la billetera en caso de pérdida, robo o fallo del dispositivo. Debe incluir opciones de copia de seguridad seguras para que los usuarios puedan restaurar su billetera y recuperar el acceso a sus activos digitales y credenciales de identidad.
- **Interoperabilidad:** Permitir una perfecta integración y comunicación con múltiples sistemas y plataformas. Esto garantiza que la billetera pueda funcionar en diferentes entornos tecnológicos y normativos, facilitando el intercambio eficiente de información, credenciales y transacciones en una economía digital global.

Las billeteras digitales universales representan un nuevo canal para las interacciones digitales, con el potencial de resolver la mayoría de los retos relacionados con la identidad digital y los pagos que afectan a cientos de millones de personas cada día, como se abordará más adelante en este documento. Esta nueva generación de billeteras también redefinirá la forma en que nos comunicamos entre nosotros y con nuestros ecosistemas, lo que a su vez dará lugar a una nueva generación de productos y servicios centrados en el usuario. Es decir, las billeteras digitales universales permitirán no solo realizar autenticación y los pagos, sino también gestionar publicidad, mensajería, fidelización o votaciones, entre otras cosas, creando nuevas experiencias de usuario y modelos de negocio.



2. Billeteras Digitales Universales y la Identidad Digital



2.1. Revisando la idea de identidad

La identidad es el conjunto de atributos y características que definen de manera única a un individuo o entidad, distinguiéndolos de los demás en un contexto determinado. Esto incluye una amplia gama de información -rasgos físicos, datos biométricos, experiencias, posesiones, relaciones, etc.- que nos hace identificables de forma única. Ser identificable de forma única es crucial para la autenticación, que implica probar la identidad de uno ante los demás demostrando la unicidad y validez de estos atributos.

La autenticación es el proceso de verificación de un conjunto de identificadores y atributos que representan a una persona o entidad. Sin embargo, dada la naturaleza cambiante de estos atributos, la captura y el almacenamiento de un conjunto completo de atributos de una persona o entidad en un único punto en el tiempo es poco práctico. En su lugar, nos basamos en subconjuntos finitos de atributos que son lo suficientemente únicos y reconocibles como para establecer nuestra individualidad.

El proceso de autenticación se basa en autoridades terceras, como gobiernos o instituciones, que expiden credenciales oficiales como pasaportes o documentos nacionales de identidad. Estos certificados proporcionan una verificación de identidad reconocida y fiable, que permite a las personas demostrar quiénes son con un alto nivel de garantía. Por normativa, las autoridades gubernamentales tienen el mandato de proporcionar y supervisar la expedición de estas credenciales oficiales para garantizar que cumplen las normas establecidas de seguridad y exactitud. Esta supervisión normativa ayuda a mantener la integridad y fiabilidad de los sistemas de verificación de identidad, reforzando la confianza pública en las credenciales utilizadas para la autenticación.

El Objetivo de Desarrollo Sostenible 16.9 de la ONU pretende proporcionar identidad legal a todos para 2030, destacando la importancia del registro de nacimientos y la documentación civil. A pesar de estos esfuerzos, aproximadamente 1.000 millones de personas en todo el mundo siguen careciendo de prueba de identidad, lo que impide su acceso a servicios y derechos esenciales. Aunque la Declaración Universal de Derechos Humanos no menciona explícitamente la "identidad", sí reconoce implícitamente la necesidad de identificación a través de derechos, como el reconocimiento legal y la nacionalidad. Garantizar que todo el mundo pueda ser identificado es fundamental para proteger estos derechos.

Actualmente, el 14% de la población global no tiene documento de identidad



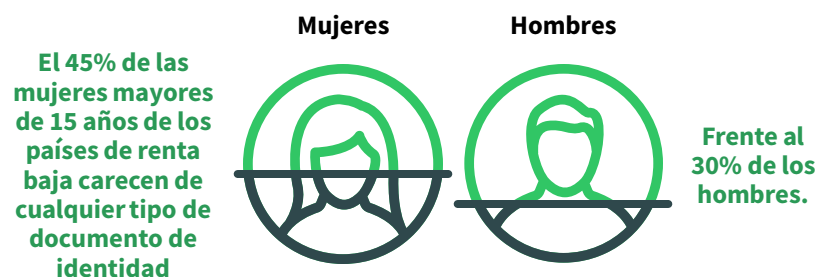
El ODS 16 para 2030 es que todo el mundo tenga identidad.

2.2. Problemas de la identificación y la autenticación

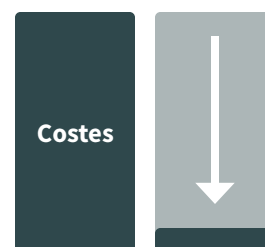
Extrapolando a lo digital el concepto de identidad, una identidad digital es un conjunto definido de atributos que permiten a los individuos ser identificables de forma única y autenticarse electrónicamente (es decir, a través de Internet). Disponemos de múltiples identidades digitales, cada una de las cuales está representada por uno o varios identificadores y un conjunto de atributos que son únicos dentro de su contexto específico.

La identidad digital permite conexiones y transacciones verificables remotas en tiempo real, así como la prestación y recepción de servicios digitales de manera segura y confiable, evitando las limitaciones del mundo físico. Los sistemas sólidos de gestión de identidades son esenciales porque nos permiten autenticarnos electrónicamente ante terceros y confiar en que la persona o empresa con la que interactuamos en línea es quien dice ser.

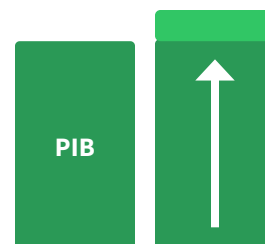
Según McKinsey&Co., una "buena identificación digital" se verifica y autentica con un alto nivel de garantía a través de canales digitales, es única, se crea con el consentimiento individual y da prioridad a la privacidad del usuario y al control sobre sus datos personales. [1] McKinsey&Co. sugiere una identificación digital con esas características impulsaría el valor y fomentaría la inclusión, como se muestra a continuación:



Con una identidad digital, **1.700 millones** de personas podrían acceder a los servicios financieros.



Con las identidades digitales, los costes de incorporación de clientes podrían reducirse hasta en un **90%.**



Las identidades digitales podrían desbloquear un valor económico que oscila entre el **3 y el 13%** del PIB en 2030, dependiendo del país.

Hoy en día, la mayoría de las personas no son dueñas de sus identidades digitales porque carecen de control sobre sus datos de identidad digital y, por lo tanto, no pueden autenticarse ante los demás autónomamente. La autenticación digital, o conseguir que otros verifiquen quiénes somos en línea, depende a menudo de terceros proveedores de identidad, sistemas de identidad federados y procesos de conocimiento del cliente (KYC por sus siglas en inglés). Estos mecanismos desempeñan un papel crucial a la hora de habilitar el acceso a los servicios digitales, pero también ponen de relieve la compleja dinámica en torno a la propiedad y el control de nuestras identidades digitales.

Cuando accedemos a servicios en línea, solemos confiar en intermediarios -como plataformas de redes sociales, servicios de correo electrónico o proveedores de servicios KYC- para verificar nuestras identidades. Estos proveedores conservan nuestros datos y credenciales y los utilizan para autenticarnos en diversos servicios. A menudo, utilizan estos datos sin nuestro conocimiento o consentimiento, con fines de monetización. No podemos hacer nada al respecto. Dependemos de ellos para gestionar, proteger y validar nuestra identidad. Estamos a merced de sus condiciones de servicio, prácticas de seguridad y cumplimiento de la normativa, con recursos limitados si algo va mal. Pero los particulares no son los únicos que sufren las consecuencias de este statu quo ineficaz. Las empresas también sufren:



Las instituciones financieras gastan
entre 20 y 40
dólares por cliente. [2]



El fraude de identidad en EE. UU.
provocó pérdidas superiores a los
23.000 millones
de dólares en 2023. [3]



Hasta el 40%
de las interacciones digitales fracasan
por problemas de identidad ¹

1 Mastercard, Restablecer la confianza en un mundo digital, 2019

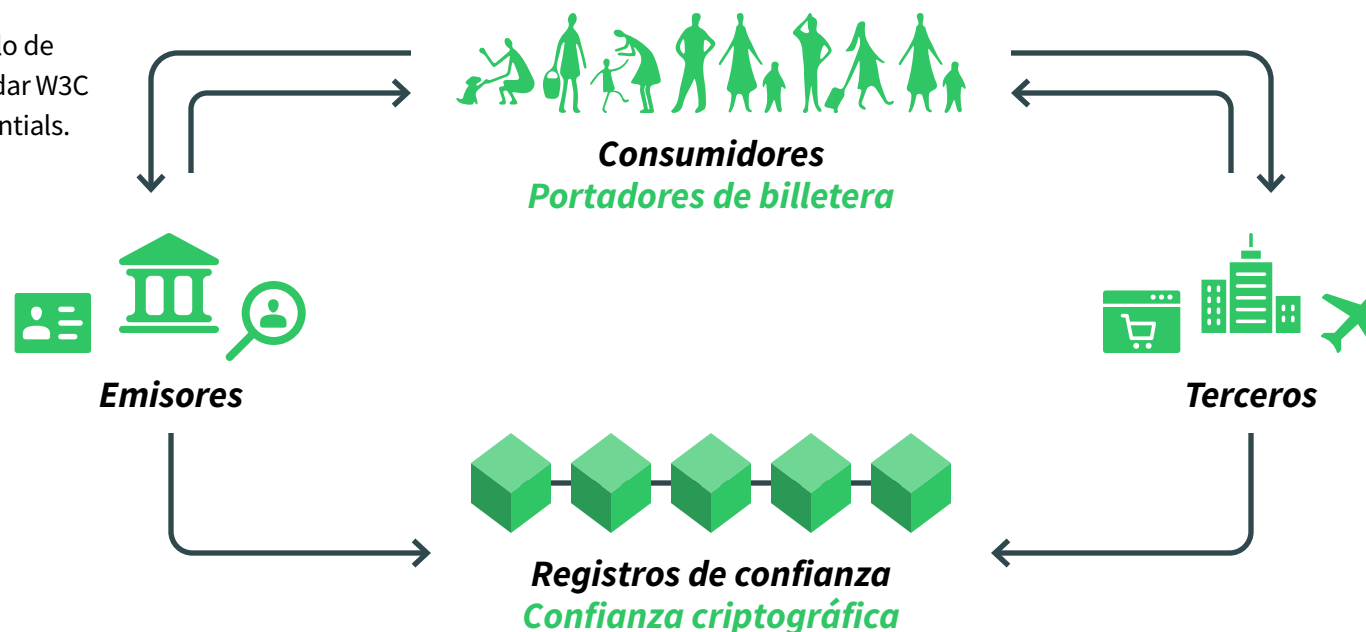
Aunque los gobiernos tienen la tarea de proporcionar los medios para la autenticación de los ciudadanos, y lo ideal sería que los ciudadanos fueran propietarios de sus propios datos y credenciales, el panorama de la identidad ha estado dominado históricamente por un ecosistema ineficiente bajo el control de terceros de carácter privado. Esto se debe en gran medida a la ausencia de tecnologías avanzadas y reglamentos adecuados que apoyen las soluciones de gestión de identidad centradas en el usuario. Sin embargo, este panorama está evolucionando. Las billeteras digitales de identidad están emergiendo como una parte crucial de la solución, facilitando un cambio hacia marcos de gestión de identidades más seguros, eficientes y centrados en el usuario.

2.3. Las billeteras digitales de identidad redefinirán la identidad digital

Las billeteras digitales de identidad son las interfaces ideales para dar a las personas el control sobre sus datos, ya que proporcionan una bóveda segura en la que almacenarlos. Permiten a los individuos ser dueños de sus identidades digitales y decidir qué información de identidad compartir, con quién y con para qué. Una solución para la identidad digital basada en billeteras digitales de identidad a través de credenciales reutilizables que son gestionadas desde las billeteras ofrece un enfoque transformador para la gestión de la identidad digital que traslada el control y la propiedad de las identidades digitales de terceros a los individuos mismos, permitiendo que los individuos gestionen sus identidades de forma segura y eficiente a través de múltiples plataformas.

En el ecosistema de las billeteras digitales de identidad, el flujo de datos involucra dos tipos de entidades: los emisores y los verificadores. Los emisores son entidades que proporcionan datos en forma de credencia-

Figura 1. Modelo de datos del estandar W3C Verifiable Credentials.



les digitales a las personas. Estas entidades pueden incluir organismos gubernamentales que expiden documentos nacionales de identidad, instituciones educativas que proporcionan diplomas e instituciones financieras que ofrecen extractos bancarios, entre muchas otras. Los verificadores, por su parte, autentican y verifican las credenciales digitales (proporcionadas por los emisores a los individuos) que éstos les presentan. Los verificadores pueden ser empleadores que realizan comprobaciones de antecedentes, proveedores de servicios que exigen una prueba de edad o bancos que garantizan el cumplimiento de las políticas KYC.

El Modelo de Datos de Credenciales Verificables del W3C (representado a continuación) -que actualmente está siendo adoptado por la Unión Europea, Estados Unidos, Canadá y múltiples organizaciones del sector privado- proporciona un marco estandarizado para gestionar e intercambiar credenciales

digitales con billeteras las digitales de identidad en el centro de la autenticación de identidad centrada en el usuario. El modelo define cómo se emiten, presentan y verifican las credenciales para garantizar la interoperabilidad y la coherencia entre las distintas plataformas y sistemas de todo el mundo.

En este modelo, la autenticidad se demuestra mediante firmas digitales o pruebas criptográficas que validan el origen y la integridad de la credencial. Esto permite a los individuos presentar sus credenciales digitales a los verificadores (como, por ejemplo, proveedores de servicios) de una manera que garantiza la privacidad y la seguridad y permite a los verificadores confirmar la autenticidad de las credenciales digitales presentadas por los individuos.

La confianza entre emisores y verificadores se intermedia a través de un registro de confianza, un sistema seguro que mantiene las pruebas de

la integridad y autenticidad de las credenciales emitidas. Mientras que las credenciales digitales (es decir, los datos) viven en la billetera, las pruebas criptográficas, las marcas de tiempo y los estados de revocación se registran en estos registros de confianza. El registro de confianza actúa como punto de referencia común que conecta a emisores y verificadores, permitiendo la verificación de la validez de las credenciales y garantizando que no han sido manipuladas, sin necesidad de interacción directa o integración entre emisores y verificadores.

Los registros de confianza pueden ser centralizados o descentralizados. Al aprovechar tecnologías como blockchain, los registros de confianza descentralizados ayudan a establecer un enlace seguro y verificable entre el titular del credencial (el individuo), la entidad emisora y el verificador. Los registros de confianza descentralizados permiten un enfoque centrado en el usuario, donde las personas pueden presentar de manera autónoma credenciales verificables desde sus billeteras a verificadores que implementan procesos de verificación que garantizan la privacidad de datos y son escalables, interoperables y confiables.

2.4. Los verificadores tienen el control último sobre la aceptación de credenciales digitales

Las implementaciones de esta nueva generación de credenciales verificables reutilizables, incluidas aquellas centrales en las regulaciones de identidad digital de la UE, prevén que las billeteras digitales contendrán

una amplia gama de credenciales verificables, extendiéndose más allá de las credenciales emitidas solo por el gobierno. La misma regulación obliga a todos los actores públicos y privados ofreciendo servicios digitales en la UE a aceptar credenciales de identidad digital emitidas por entidades gubernamentales o Proveedores de Servicios de Confianza (TSPs), incluidos los proveedores certificados de identificación.

En cuanto a las credenciales no emitidas por entidades de gobierno, el verificador sí tiene la capacidad de decidir si las acepta como válidas o no, lo que vendrá típicamente determinado por su grado de confianza en el emisor de la misma. Estas credenciales verificables no gubernamentales, como diplomas, certificados profesionales o títulos de propiedad, entre otros, son respaldadas y vinculadas a atestaciones emitidas por entidades que dan fe de la confiabilidad y validez de la credencial. Así que, asumiendo por el bien del argumento que, después de verificar la credencial (utilizando la tecnología aplicable), el verificador todavía tiene dudas sobre la credencial debido, por ejemplo, a que no conocen (o confían en) al emisor, el verificador puede rechazar la credencial.

En otras palabras, las partes que confían (verificadores) siempre pueden decidir si confían o no en los datos contenidos en la credencial digital. En última instancia, esta determinación se basará en su evaluación sobre la confiabilidad de la parte emisora. Si una credencial es verificable y válida, pero fue emitida por alguien o alguna entidad que el verificador considera poco confiable, el verificador no estaría obligado a aceptar dicha credencial. De manera significativa, las funcionalidades relacionadas con el proceso de verificación se automatizarán, permitiendo que los verificadores establezcan reglas sobre qué tipos de credenciales y emisores están dispuestos a aceptar. Estas reglas asegurarán que los verificadores puedan aceptar solamente aquellas credenciales de emisores en los que confían y rechazar las demás.

El Punto de Verificación (PoV) es una parte clave de cómo las organizaciones a las que nos hemos venido refiriendo como verificadores configuran reglas personalizadas para la verificación de credenciales. Los PoVs son como la versión de identidad de los terminales de pago (POS) que vemos en tiendas o en línea. Permiten a las organizaciones crear interfaces presenciales o digitales donde les presentan a los una solicitud para autenticarse (por ejemplo en forma de QR) y estos responden compartiendo las credenciales necesarias desde su billetera. Este proceso hace que la verificación de identidad sea segura y eficiente. En los próximos años, veremos la mayoría de los sitios web incorporando PoVs que muestren un código QR que permita a los usuarios autenticarse “conectando sus billeteras.” Esto significa que los usuarios compartirán una credencial específica desde su billetera para verificar su identidad de manera rápida y segura. Los accesos físicos a eventos, estadios y edificios también incorporarán PoVs compatibles con tecnologías QR y NFC.



3. Transferencia de valor y billeteras digitales universales



3.1. Las ineficiencias de los sistemas actuales

La transferencia de valor -el proceso de mover activos, fondos o cualquier forma de valor de una entidad a otra- es fundamental para la economía mundial. Sin embargo, en la era digital, los procesos de transferencia de valor se enfrentan a varios retos que afectan a la eficiencia, la seguridad y la accesibilidad. Estos problemas van desde las limitaciones tecnológicas y los obstáculos normativos hasta la preocupación por la privacidad y la confianza.

El panorama actual de la transferencia de valor está muy fragmentado. Se utilizan múltiples sistemas y redes para transferir valor a través de fronteras, divisas y plataformas. Esta fragmentación genera complejidad y hace que las transacciones sean lentas, caras y propensas a errores. Por ejemplo, en los pagos transfronterizos suelen intervenir varios intermediarios, lo que deriva en costes y retrasos. La dependencia de la infraestructura bancaria tradicional para estas transferencias también puede excluir a quienes no tienen acceso a instituciones financieras.

Transferir valor, especialmente de manera transfronteriza, puede resultar caro. Las comisiones por cambio de divisas, los bancos intermediarios y el cumplimiento de la normativa local pueden reducir considerablemente la cantidad recibida por el destinatario. Por ejemplo, las comisiones por envío de remesas, que a menudo recaen sobre las poblaciones más vulnerables, pueden mermar los limitados fondos que los trabajadores emigrantes envían a sus familias. El Banco Mundial calcula que el coste medio del envío de remesas en todo el mundo ronda el 6-7% del valor transferido, y algunos corredores cobran tasas mucho más elevadas.

A medida que la transferencia de valor ocurre más y más de forma digital, los ciberdelincuentes se centran en los puntos débiles de los sistemas de pago,

lo que provoca importantes pérdidas financieras. En 2023, las pérdidas mundiales por fraude en los pagos se estimaron en más de 40.000 millones de dólares, [4] lo que pone de manifiesto las vulnerabilidades de los sistemas. Garantizar transacciones seguras requiere de cifrado robusto, medidas de autenticación y una vigilancia constante contra las amenazas emergentes.



En 2023, las pérdidas mundiales por fraude en los pagos se estimaron en más de

40.000 millones
de dólares.



1/3

de la población mundial carece de acceso a cualquier tipo de servicio financiero.

Mientras que las personas con acceso a servicios financieros se enfrentan a todas las limitaciones mencionadas, 1/3 de la población mundial carece de acceso a cualquier tipo de servicio financiero. Esta falta de inclusión financiera les impide participar en los sistemas de transferencia de valor, lo que limita sus oportunidades económicas. Por ejemplo, en muchos países en desarrollo, las personas recurren a canales informales para transferir valor, que suelen ser menos seguros y más caros que los sistemas financieros formales.

3.2. Pagos digitales y tokenización de activos

La introducción de Bitcoin en 2008, y las muchas otras criptomonedas que le siguieron después, supuso un cambio revolucionario en la forma de realizar pagos y transacciones financieras. El sistema financiero mundial está dominado por intermediarios de confianza que habilitan los canales de transferencia de valor. Estas instituciones controlan la infraestructura, el flujo de fondos y, en consecuencia, la accesibilidad de los servicios financieros.

Bitcoin desafió este statu quo al proponer una moneda digital descentralizada que funciona en una red entre pares sin necesidad de que autoridades terceras validen las transacciones y garantizando la fidelidad de los pagos y la liquidación de las transferencias de valor casi en tiempo real. Bitcoin introdujo una solución sólida para un registro de confianza descentralizado, una red blockchain, que permite un registro público cronológico e inmutable de las transacciones.

A medida que la tecnología blockchain ganaba terreno, un concepto más amplio de tokenización surgió como una aplicación transformadora en muchos sectores. La tokenización consiste en representar derechos de propiedad o valor en paquetes digitales de datos, denominados tokens, que se registran en una cadena de bloques. Estos tokens pueden representar una amplia gama de activos, como monedas digitales, bienes inmuebles, valores financieros, materias primas y activos intangibles como la propiedad intelectual. Al crear representaciones digitales de estos activos, la tokenización ofrece una nueva forma de gestionar, comerciar y verificar la propiedad de manera digital.

Este cambio ha catalizado profundos avances en el sector financiero, en particular mediante el fomento de un renovado interés en las monedas digitales

y la aplicación más amplia de la tecnología blockchain para modernizar los sistemas de pago. Las instituciones financieras de todo el mundo reconocen ahora el enorme potencial de la tokenización para agilizar y asegurar las transacciones transfronterizas. Al aprovechar la tokenización, estas instituciones pueden lograr tiempos de transacción más rápidos, costes de procesamiento reducidos y una mayor transparencia, elementos que generan confianza y eficiencia. Esta evolución no sólo simplifica el proceso de transacción, sino que también abre nuevas vías para la innovación financiera, desafiando los marcos bancarios tradicionales y sentando las bases para una economía global más interconectada y eficiente.

La tokenización mejora el sistema financiero al garantizar que los servicios estén disponibles 24 horas al día, 7 días a la semana, permitiendo que las operaciones y transacciones se produzcan en tiempo real y a escala mundial. Cuando los activos y los pagos se convierten en tokens digitales, se intercambian en un libro de contabilidad descentralizado como blockchain, que actúa como un registro de confianza común. Esto significa que todas las partes tienen acceso a la fuente de la verdad y que cada transacción se procesa, registra y verifica de forma segura y transparente.

El método de liquidación conocido como entrega contra pago (DvP, por su nombre en inglés), que garantiza que los activos sólo se transfieren una vez efectuado el pago, se vuelve mucho más eficiente con la tokenización porque permite el intercambio simultáneo de tokens que representan activos, contra tokens que representan pagos. Como resultado, las transacciones pueden liquidarse inmediatamente, reduciendo el riesgo de que una de las partes no cumpla su parte del trato (también conocido como riesgo de contraparte).

Además de hacer las transacciones más rápidas y seguras, la tokenización también ayuda a reducir costes. Al utilizar la blockchain como libro de contabilidad de confianza, se reduce la necesidad de intermediarios y se agilizan muchos de los procesos manuales que intervienen en las transacciones financieras tradicionales. Esto crea un flujo de transacciones más directo y eficiente, ahorrando tiempo y dinero.

Varias instituciones financieras y gestores de activos ya han comenzado a utilizar la tecnología blockchain para emitir, comprar y vender tokens digitales que representan activos del mundo real. En 2023, JP Morgan gestionó más de 1.000 millones de dólares de transacciones diarias utilizando su token digital JPM coin como parte de su visión estratégica, que reconoce que la tecnología blockchain puede ayudar a las instituciones financieras a dar el salto a una infraestructura que admite transacciones casi instantáneas y automatiza la complejidad. [5] Además, el 75% de los principales clientes de instituciones bancarias y financieras de Fireblocks están explorando la tokenización. Excluyendo las criptomonedas y las *stablecoins*, McKinsey, Citi Group y Boston Consulting Group estiman que para 2030, el valor de mercado de los activos financieros tokenizados será de 2,000 millones de dólares, [6] 4,000 millones de dólares [7] y 16,000 millones de dólares, [8] respectivamente, representando esta última estimación el 10% de todos los activos financieros en circulación.²



En 2030, el volumen de activos tokenizados será entre
\$2 y \$16 trillones
representando un
10%
del total de activos financieros.

Los bancos centrales también han empezado a desarrollar monedas fiduciarias digitales (denominadas monedas digitales de bancos centrales, CBDC, por nombre en inglés) para modernizar su infraestructura de pagos. Las CBDC ofrecen a los bancos centrales la eficiencia de las criptomonedas y, al mismo tiempo, el control de su política monetaria. Más de 130 países, que representan el 98% del PIB mundial, están estudiando actualmente la posibilidad de implantar una CBDC. Esto incluye diecinueve de los 20 países del G20. Bahamas, Jamaica y Nigeria ya han puesto en marcha su propio CBDC. [9]

3.3. Billeteras digitales universales para redefinir la transferencia de valor

Las billeteras digitales universales están llamados a transformar el panorama de la transferencia de valor combinando hábilmente los métodos de pago tradicionales con la tokenización innovadora y la verificación avanzada de la identidad. Estas billeteras facilitan la gestión y transferencia de una amplia gama de activos, desde criptomonedas y activos reales tokenizados, como bienes inmuebles y acciones, hasta transacciones convencionales con tarjetas de crédito y débito. Como interfaces seguras, contienen claves privadas esenciales para acceder a estos activos digitales y sirven como puertas de entrada absolutamente necesarias a los ecosistemas financieros tokenizados emergentes.

2. Una *stablecoin* es un tipo de criptomoneda diseñada para tener un valor estable al estar vinculada a una reserva de activos, como una moneda fiduciaria como el dólar estadounidense, u otros instrumentos financieros como materias primas o una cesta de criptomonedas.

Una característica transformadora de las billeteras digitales universales es la integración de credenciales digital para la verificación de la identidad. Este desarrollo va más allá de los métodos biométricos tradicionales, proporcionando defensas sólidas contra la evolución del fraude de identidad digital con Inteligencia Artificial. Las *personhood credentials*, que incluyen elementos como huellas digitales y patrones de comportamiento, mejoran los procesos de KYC, permitiendo a los usuarios verificar sus identidades sin problemas y sin enviar repetidamente datos personales a diferentes proveedores de servicios. Esto no solo simplifica las transacciones financieras, sino que también mejora la privacidad y el control sobre los datos personales, permitiendo a los usuarios gestionar sus identidades y actividades financieras en un marco seguro.

Este enfoque integral permite a los usuarios interactuar en múltiples plataformas y servicios de forma segura, transfiriendo activos digitales y realizando pagos tradicionales sin esfuerzo desde una única interfaz de billetera. Por ejemplo, los usuarios pueden aprovechar sus billeteras para realizar compras utilizando sus tarjetas de débito o crédito vinculadas, invertir en mercados internacionales o participar en transacciones seguras entre pares sin intermediarios. Además, este control directo puede democratizar el acceso al sistema financiero mundial, beneficiando especialmente a las personas de regiones desatendidas que pueden carecer de acceso bancario tradicional, pero que ahora pueden participar en la economía digital.

Además, las billeteras digitales universales facilitan la distribución eficiente de ayuda gubernamental u organizacional y subsidios directamente a los destinatarios. Este enfoque directo minimiza la carga administrativa, reduce las oportunidades de fraude y garantiza la entrega oportuna de asistencia a quienes la necesitan, mejorando así la efectividad de los programas de bienestar social.

La adopción de Puntos de Verificación (PoV), como se introdujo en la Sección 2.4, se convertirá en los endpoints para las nuevas pasarelas de pago. Las billeteras digitales permitirán a los individuos gestionar de manera segura sus identidades digitales y pagos, respondiendo a solicitudes de autenticación y pago mediante el escaneo de un código QR o mediante tecnología NFC. La evolución de los POS actuales a PoV para identidad y pagos permitirá prevenir el fraude creciente en la autenticación digital y los pagos, al inhibir el uso de inteligencia artificial para el fraude de identidad a través de ataques de fuerza bruta de contraseñas o falsificación en verificaciones biométricas. Con la autenticación y pagos basados en PoVs, que solo permiten iniciaciones desde billeteras digitales, las contraseñas y verificaciones biométricas ya no son necesarias, y la seguridad aumenta exponencialmente.

En conclusión, al integrar métodos de pago tradicionales, pagos tokenizados y tecnologías avanzadas de verificación de identidad, las billeteras digitales universales no solo simplifican la experiencia del usuario, sino que también abren puertas a la inclusión financiera y a la innovación en el comercio global, marcando un paso significativo en la evolución de las finanzas digitales, donde la seguridad, la privacidad y la autonomía del usuario se logran.



4. El camino hacia las billeteras digitales universales



En general, las billeteras digitales de hoy en día pueden caracterizarse como billeteras de pago o billeteras de identificación. Las billeteras de pago como PayPal, Google Pay, Apple Pay, Alipay y WeChat han logrado una adopción masiva en todo el mundo, con más de 13,9 billones (miles de millones) de dólares en transacciones en 2023. Las proyecciones sugieren que esta cifra podría duplicarse en 2027. Estas billeteras han revolucionado la forma en que los consumidores realizan pagos y han agilizado las transacciones en innumerables plataformas en distintas geografías.

Del mismo modo, las billeteras digitales, a menudo impulsados por iniciativas gubernamentales, han experimentado una adopción significativa en múltiples regiones. Países como India, Estonia y Singapur han abierto el camino con versiones de lo que puede considerarse "eWallets 1.0", o "billeteras electrónicas gubernamentales 1.0". Estas billeteras digitales se integran con diversos servicios públicos y ofrecen a los ciudadanos un medio digital para acceder a los servicios sociales, pero su integración con los servicios del sector privado sigue siendo limitada y no existe interoperabilidad transfronteriza.

El concepto de billetera digital universal representa la convergencia de las funciones de pago e identidad en un único canal centrado en el usuario. Estas billeteras no sólo pueden gestionar transacciones financieras, sino también gestionar y verificar de forma segura las identidades y credenciales de los usuarios. Este enfoque integrado promete simplificar las interacciones de los usuarios con los servicios públicos y privados a escala digital, proporcionando una experiencia de usuario más holística y eficiente.

El nuevo modelo de la Unión Europea y el reglamento correspondiente aprobado por la Comisión Europea en 2024 para las billeteras de identificación tienen el potencial de servir de modelo para el futuro de las billeteras digitales universales. El marco de la UE está diseñado para fomentar un mercado de datos que podría reproducirse a escala mundial. Al permitir a los usuarios controlar su información personal y financiera de forma segura

y cómoda, estas billeteras están preparados para redefinir los límites entre la verificación de la identidad y los procesos transaccionales.

El modelo se basa en normas y protocolos abiertos desarrollados por organizaciones internacionales como OpenID, W3C e ISO, que son fundamentales para la interoperabilidad transfronteriza. Se prevé que, a medida que avance su adopción, el modelo de la UE fomentará un floreciente ecosistema que se beneficiará de múltiples efectos de red (*network effects*, en inglés). Además, los mandatos gubernamentales que obligan al sector privado a aceptar billeteras de identificación para la autenticación, junto con los esfuerzos para establecer un entorno regulado para los proveedores de billeteras digitales, impulsarán aún más la adopción generalizada.

La siguiente sección, dividida en tres subsección, destaca los avances e identifica los huecos que deben cubrirse para alcanzar todo el potencial de la tecnología de billeteras digitales. En primer lugar, se presentan varias de las implementaciones más exitosas de la primera generación de billeteras de identificación gubernamentales -eWallets 1.0. A continuación, exploramos los avances de la segunda generación de billeteras digitales en desarrollo en la Unión Europea, Estados Unidos y Canadá, denominados eWallets 2.0. Por último, analizamos los componentes necesarios para que las eWallets 2.0 se conviertan en las billeteras digitales universales superiores que impulsarán la economía digital mundial.

4.1. eWallets 1.0

Existen algunos casos de éxito en la implantación gubernamental de billeteras digitales que ofrecen a los ciudadanos un acceso simplificado a los servicios públicos, así como una interoperabilidad limitada pero al menos existente con el sector privado. Tres soluciones han sido reconocidas en todo el mundo: Estonia, India y Singapur. Analizar estas soluciones y las

lecciones aprendidas resulta útil para estudiar la mejor manera de desarrollar la próxima generación de billeteras digitales.

4.1.1. Estonia

Estonia es considerada líder mundial en gobernanza digital, y su iniciativa e-Estonia sirve de modelo para otras naciones. La piedra angular del ecosistema digital de Estonia es su programa de residencia electrónica y su documento de identidad digital, que funciona como una billetera digital completa para ciudadanos y residentes. Se calcula que el 99% de sus servicios públicos están disponibles 24 horas al día, 7 días a la semana. [10]

X-Road es la plataforma de intercambio de datos descentralizada de Estonia que sustenta los servicios digitales del país. Permite que varios sistemas y bases de datos se comuniquen entre sí de forma segura y eficiente. X-Road facilita el intercambio seguro de datos entre diferentes organizaciones y sistemas, incluidos organismos gubernamentales, entidades del sector privado e instituciones públicas. Permite a estas entidades acceder a la información y compartirla en tiempo real.

La tarjeta de identidad de Estonia, vinculada al número de identidad único de una persona, permite acceder a más de 600 servicios electrónicos, como banca, sanidad, votaciones y otros. La tarjeta contiene un microchip que almacena de forma segura certificados digitales de autenticación y firmas digitales que permiten a los usuarios acreditar su identidad y firmar documentos electrónicamente. Estonia tiene previsto integrar su ID digital con una billetera digital mejorada que se ajuste a la nueva normativa europea, de la que hablaremos más adelante.

4.1.2. India

Los sistemas de identidad y billetera digitales de la India son el mayor y más ambicioso proyecto de infraestructura digital a escala mundial, encabezado

principalmente por el Gobierno indio a través de las iniciativas Aadhaar y el Programa Digital de India.

Aadhaar es la columna vertebral del ecosistema de identidad digital de la India. Lanzado en 2009 por la Autoridad de Identificación Única de la India, Aadhaar proporciona un número de identificación único a cada residente en la India. Está diseñado para facilitar el acceso a diversos servicios y prestaciones.

Cada número Aadhaar es un identificador único de 12 dígitos vinculado a datos biométricos (huellas dactilares y escaneo de iris) y demográficos (nombre, dirección, fecha de nacimiento). Aunque la inscripción en Aadhaar es voluntaria, se fomenta mucho y se ha convertido en una identidad de facto para acceder a una amplia gama de servicios.

Aadhaar proporciona servicios de autenticación mediante verificación biométrica, que se utiliza para validar la identidad en diversas transacciones y servicios, como la apertura de cuentas bancarias o el acceso a subvenciones públicas. Los datos de Aadhaar se almacenan en una base de datos segura y su acceso está controlado. El sistema incorpora varias medidas de seguridad para proteger los datos personales, aunque ha habido preocupación por la privacidad y las violaciones de datos. En 2023, un hackeo logró robar y exponer en la dark web la información de identificación personal de 815 millones de indios. [11]

4.1.3. Singapur

SingPass es el principal sistema de identidad digital de Singapur, que ofrece a los ciudadanos una forma segura de acceder a los servicios de la Administración y del sector privado. SingPass proporciona una identidad digital única que permite a los usuarios iniciar sesión en diversos portales y servicios gubernamentales, como la declaración de impuestos, los servicios sanitarios y los sistemas de transporte público.

Según el Gobierno de Singapur y el Banco Mundial, el 97% de la población que cumple los requisitos (equivalente a 4,5 millones de ciudadanos y residentes) utiliza la aplicación Singpass para acceder en línea a más de 2.000 servicios de los sectores público y privado, desde servicios financieros a sanidad, educación, servicios empresariales y transporte. Cada año se realizan más de 350 millones de transacciones, y trámites que antes tardaban días u horas y a menudo requerían visitas físicas, ahora se realizan en minutos y desde cualquier lugar con conexión a internet. Recientemente se ha añadido una billetera de documentos que permite a los ciudadanos y residentes guardar sus documentos de identidad, licencias de conducir y documentación de vacunación COVID-19, entre otros documentos.

APEX, una interfaz de programación de aplicaciones (API) para que los organismos públicos compartan y reutilicen datos de forma transparente, segura y sin fisuras, ha permitido que los servicios públicos sean más eficientes. Más de 2.000 servicios de más de 45 proyectos de agencias diferentes, aproximadamente la mitad de todas las agencias gubernamentales de Singapur, utilizan la API APEX. El nivel de tráfico ha superado los 100 millones de transacciones al mes, con picos que superan por término medio los 300 millones de transacciones mensuales.

La colaboración entre el gobierno de Singapur y el Banco Mundial, que elaboró un análisis exhaustivo de Singpass, identificó algunas áreas importantes de mejora, entre ellas:

- **Descentralización y registros de confianza alternativos:** Exploración del potencial de los modelos de identidad federados y descentralizados para Singpass. Recomendamos también la consideración de registros de confianza alternativos, en particular para un modelo descentralizado en el que los datos del usuario pueden no obtenerse directamente de una interfaz de programación de aplicaciones (API), sino más bien ser compartidos por el usuario directamente con un servicio.
- **Autorización:** Utilización de Singpass como medio para que los clientes autoricen a distancia las transacciones basándose en la sólida autenticación y verificación de usuarios que proporciona el sistema de número de identidad único (DNI), y no solo para la inscripción, como funciona actualmente. Un ejemplo podría ser una notificación push de una aplicación bancaria para autorizar un pago.
- **Ampliación de la billetera digital:** Incorporar una mayor variedad de credenciales de identidad, como las licencias de conducir expedidas por el gobierno y las tarjetas de identificación militar; tarjetas relacionadas con la profesión, como los carnés de conducir comerciales y las certificaciones de médicos; tarjetas relacionadas con prestaciones, como las expedidas para subsidios sanitarios o para personas mayores.
- **Delegación:** Habilitar que particulares interactúen con la Administración y las empresas no solo por sí mismos sino también en nombre de otros, como padres ancianos y familiares con menos conocimientos digitales. Se ha comprobado que las familias hoy en día comparten contraseñas claves de la persona en cuyo nombre realizan la transacción, lo cual es inseguro e inconveniente. Singapur está estudiando la forma de integrar la delegación digital en Singpass, de modo que los usuarios puedan delegar con mayor seguridad en familiares de confianza para que realicen transacciones digitales en su nombre.
- **Interoperabilidad transfronteriza:** Explorar casos de uso transfronterizo de la identidad digital.
- **Ampliación de APEX para el sector privado:** Apoyar los casos de uso de gobierno a ciudadano (G2C) y de gobierno a empresa (G2B).

4.1.4. Lecciones aprendidas de las eWallets gubernamentales 1.0

Las billeteras digitales ofrecidos por Estonia, India y Singapur han tenido éxito en varios aspectos. También han dejado áreas de mejora y desarrollo futuro, como se describe a continuación:

Eficacia y comodidad	✓	Mejora significativa de la eficiencia y la comodidad para acceder a los servicios públicos y realizar transacciones. Al integrar los organismos públicos mediante API, tanto los usuarios de billeteras como terceros pueden conectarse con múltiples servicios y bases de datos.
Accesibilidad	✓	Los servicios de la Administración son siempre accesibles, lo que permite a los ciudadanos gestionar sus asuntos a su conveniencia, independientemente de las zonas horarias o los horarios de oficina. Esto es especialmente beneficioso para expatriados, viajeros y habitantes de zonas remotas.
Notificaciones	✓	Notificaciones y actualizaciones en tiempo real sobre asuntos críticos para el ciudadano como plazos fiscales, fechas de elecciones o desembolsos de prestaciones. Esta rapidez ayuda a los ciudadanos a mantenerse informados y actuar a tiempo.
Inclusión financiera	—	La inscripción en instituciones financieras mediante billeteras digitales permite a las poblaciones vulnerables beneficiarse de ayudas financieras y acceder al sistema financiero. Sin embargo, este caso de uso ha tenido una adopción limitada.
Sector privado	—	Aunque estas billeteras permiten la interoperabilidad con el sector privado, la necesidad de integraciones independientes con la infraestructura del sector público limita la adopción y la escalabilidad.
Seguridad	—	El hecho de que terceros tengan que interactuar con las bases de datos de la Administración para verificar o consumir datos de los ciudadanos genera puntos de fallo únicos. Un enfoque centrado en el usuario minimizaría el potencial de filtración de datos.
Escalabilidad	—	Al igual que en el caso de la seguridad, el hecho de que todos los terceros interoperen de API a API no es escalable cuando cientos de miles de organizaciones pretenden prestar servicios digitales a los ciudadanos.
Interoperabilidad transfronteriza	—	La interoperabilidad transfronteriza exige un modelo que no esté centralizado. Los registros de confianza descentralizados que pueden verificar pruebas criptográficas de datos son ideales para la escalabilidad y la interoperabilidad transfronteriza.
Activos tokenizados	✗	No está diseñado para interactuar con la nueva generación de activos tokenizados.

5. eWallets 2.0



La Unión Europea ha sido pionera en un modelo de identificación que se basa en el éxito previo de las eWallets 1.0 y la mejora de sus limitaciones. Este modelo propone un enfoque centrado en el usuario en el que los individuos controlan su identidad digital en forma de credenciales reutilizables que se almacenan en una billetera digital, en su teléfono móvil. Los individuos pueden revelar sus datos de identidad a terceros directamente, a su discreción, y las credenciales que contienen estos datos pueden ser verificadas criptográficamente. Este modelo resuelve los problemas de seguridad, escalabilidad e interoperabilidad transfronteriza de las eWallets 1.0. Estados Unidos no ha adoptado este enfoque a nivel federal. Sin embargo, algunos estados han empezado a seguir un planteamiento similar con respecto a las eWallets basado en los mismos protocolos y normas abiertos que ha adoptado la Unión Europea. Canadá también se está alineando muy estrechamente con la nueva normativa europea sobre identidad y billeteras, y ha creado un Marco de Confianza Pancanadiense de Identidad Digital que se ha convertido en una referencia mundial. [12]

5.2.1. Unión Europea

Desde la década de 2000, la Comisión Europea ha tratado de desarrollar un ecosistema digital sólido que sitúe a la UE como líder digital mundial. El eje de esta visión ha sido el marco europeo de identidad digital ("eID"), un sistema normativo sostenible que permite interacciones digitales seguras, confidenciales y sin fisuras. El marco eID garantiza el reconocimiento mutuo de los sistemas nacionales de identificación electrónica en todos los Estados miembros, permitiendo a los ciudadanos de la UE identificarse y autenticarse en línea con un documento de identidad electrónico.⁷ En julio de 2014, este marco se incorporó a un nuevo y ambicioso reglamento para las interacciones electrónicas, el Reglamento eIDAS (identificación electrónica, autenticación y servicios de confianza).

Aunque los servicios electrónicos regulados funcionan muy bien en toda Europa para determinados casos de uso, las tarjetas de identidad electrónicas nunca dieron lugar a una adopción sólida por falta de seguridad, comodidad

y utilidad. Durante una década, la Comisión Europea exploró alternativas para hacer frente a estos retos. En junio de 2021, la Comisión Europea presentó una propuesta de modificación de la normativa eIDAS, urgida por las ineficiencias en la identificación digital y la verificación de credenciales que la pandemia COVID-19 puso al descubierto.

La enmienda reconocía que: "el actual Reglamento eIDAS no está a la altura de las nuevas demandas del mercado, debido sobre todo a sus limitaciones inherentes al sector público, las escasas posibilidades y la complejidad para que los proveedores privados en línea se conecten al sistema, su insuficiente disponibilidad de soluciones de identificación electrónica notificadas en todos los Estados miembros y su falta de flexibilidad para dar soporte a una variedad de casos de uso. Además, las soluciones de identidad que quedan fuera del ámbito del eIDAS, como las que ofrecen los proveedores de redes sociales y las entidades financieras, plantean problemas de privacidad y protección de datos. No pueden responder eficazmente a las nuevas demandas del mercado y carecen del alcance transfronterizo necesario para atender necesidades sectoriales específicas en las que la identificación es delicada y requiere un alto grado de certidumbre." [13]

La enmienda propuso el desarrollo de un nuevo marco europeo de identidad digital con el objetivo de que "al menos el 80% de los ciudadanos puedan utilizar una solución de identidad digital para acceder a servicios públicos clave de aquí a 2030". También propuso "un alto nivel de seguridad con respecto a todos los aspectos de la provisión de identidad digital, incluida la emisión de una Billetera Europea de Identidad Digital, y la infraestructura para la recogida, almacenamiento y divulgación de datos de identidad digital".

El debate que siguió a la modificación condujo a la elaboración del Reglamento eIDAS2, que incorpora el nuevo Marco Europeo de Identidad y una arquitectura de referencia para las billeteras EUDI (Identidad Digital de la Unión Europea). Dicho Reglamento establece tres conceptos básicos para una identidad digital centrada en el usuario que pueda interoperar con el sector público y privado en la Unión Europea y fuera de sus fronteras:

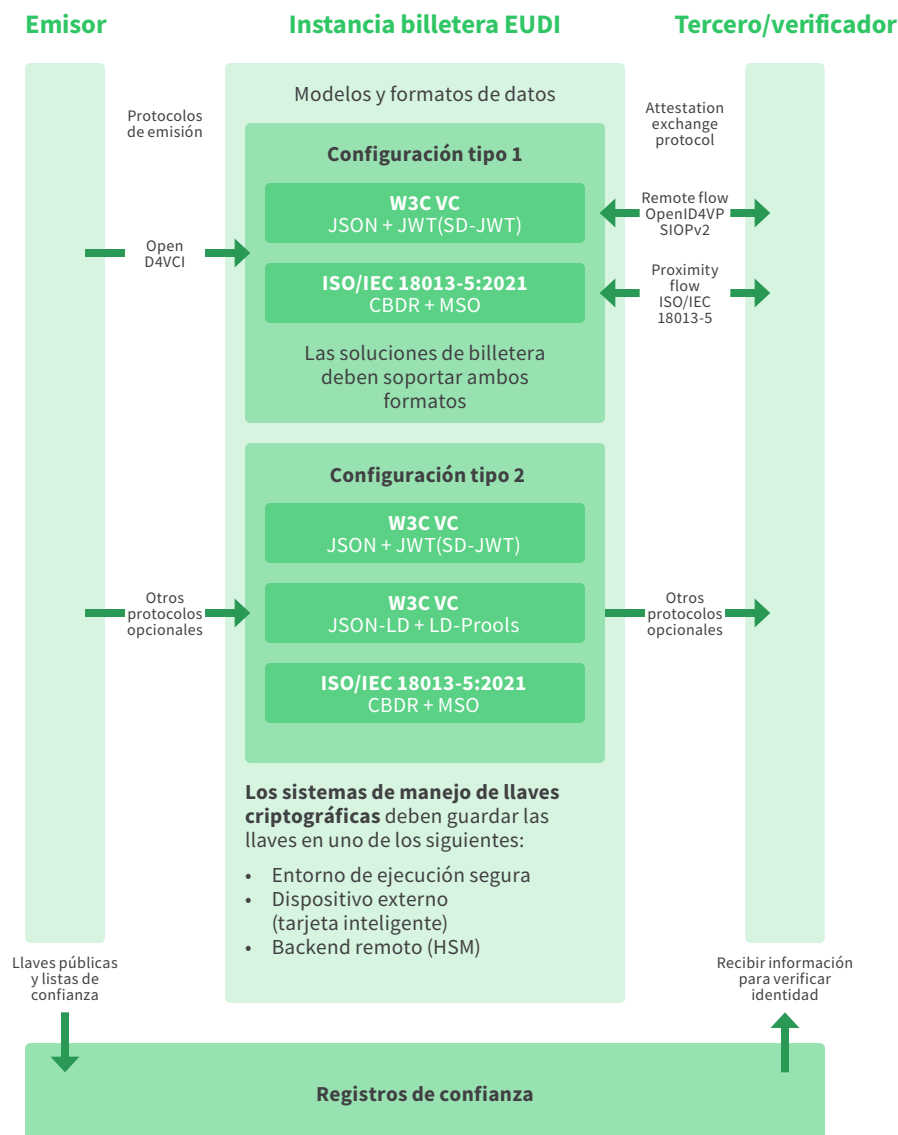
- Credenciales digitales basadas en estándares abiertos con parámetros flexibles que utilizan normas de ISO [14], W3C [15] y OpenID [16].
- Billeteras móviles de identificación que sirvan de interfaces de usuario seguras y cómodas para los ciudadanos.
- Libros electrónicos de contabilidad que facilitan la interoperabilidad y la escalabilidad.

Para garantizar la adopción masiva, de conformidad con el Reglamento eIDAS2, cada Estado miembro debe poner a disposición de sus ciudadanos al menos una billetera de identidad digital antes de 2026 y reconocer las billeteras EUDI emitidos por otros Estados miembros. [17] Adicionalmente, el Reglamento exige a las empresas del sector privado, incluidas las entidades financieras, que acepten estas billeteras digitales para autenticar la identidad de los ciudadanos de los Estados miembros.

El liderazgo de la Unión Europea en materia de identidad digital no consiste únicamente en establecer normas dentro de sus fronteras; también invita a otras regiones a interoperar con sus sistemas. El marco eIDAS2 sirve de modelo que otras regiones pueden adoptar o con el que pueden alinearse, sentando las bases para un ecosistema mundial de identidad digital en el que jurisdicciones fuera de la UE puedan participar estableciendo acuerdos de reconocimiento mutuo y garantizando el no repudio de sus credenciales digitales.

Los agentes del sector privado de la Unión Europea pronto empezarán a aceptar las billeteras digitales de identidad como algo habitual, por mandato de la Comisión Europea. Se trata de un paso importante hacia el uso de billeteras digitales de identidad a escala mundial. Esta disposición a utilizar sistemas de identidad digital similares fuera de Europa tiene implicaciones significativas, tanto para el sector privado como para el desarrollo más amplio de las billeteras digitales en todo el mundo, y sienta las bases para el crecimiento y el desarrollo de una economía digital mundial fuerte, inclusiva y en plena expansión.

Figura 2. Marco de tres actores -emisor, sujeto, tercero/verificador- para interacciones digitales centradas en el usuario, destacando estándares y protocolos propuestos por la Arquitectura EUDI Wallet Europea.



5.2.2. Estados Unidos y Canadá

A diferencia de la Unión Europea, Estados Unidos carece de una normativa federal unificada o de una infraestructura digital para la autenticación de la identidad. Sin embargo, el Departamento de Seguridad Nacional [18], así como varios estados [19], han empezado a poner a prueba billeteras de identidad digital y credenciales digitales en colaboración con proveedores del sector privado, utilizando las mismas normas que se utilizan en Europa, a saber, las normas W3C, OpenID e ISO. Las credenciales digitales basadas en estas normas abiertas permitirán la interoperabilidad entre la Unión Europea y Estados Unidos.

Además, Canadá se ha convertido en líder del desarrollo de eWallets 2.0 con su Marco Pancanadiense, que se basa en las mismas normas abiertas. El marco pretende empoderar a los ciudadanos y consumidores garantizando que las billeteras digitales se adhieran a los principios básicos de los derechos humanos, en particular los relacionados con la privacidad y el control individual sobre la información personal. El marco hace hincapié en la necesidad de una solución de identidad digital coherente y de experiencias automatizadas basadas en el consentimiento en todos los participantes del ecosistema nacional, incluidos los agentes de los sectores público y privado.

5.2.3. Ventajas de las eWallets 2.0

Eficiencia y Conveniencia	✓	Igual que eWallets 1.0.
Accesibilidad	✓	Igual que eWallets 1.0.
Notificaciones	✓	Igual que eWallets 1.0.
Inclusión Financiera	✓	Hacer obligatoria la aceptación de billeteras de identificación por parte de instituciones financieras -entre otras organizaciones- y habilitar el uso de estas billeteras para la distribución de ayuda y subsidios. Se espera que tenga un alto impacto en la inclusión financiera.
Seguridad	✓	El modelo centrado en el usuario devuelve el control al individuo. Esto minimiza la exposición de bases de datos centralizadas a terceros, reduciendo los riesgos de vulnerabilidades y puntos de fallo únicos. Los usuarios pueden controlar cuándo y a quién divulgan la información de identidad, y las capacidades de seguimiento les permiten ver quién ha accedido a sus datos.
Escalabilidad	✓	La arquitectura aprovecha nuevos registros de confianza y registros de confianza más accesibles, como los libros electrónicos descentralizados, para mejorar la verificabilidad de credenciales digitales. Esto respalda una infraestructura escalable que puede acomodar el creciente número de usuarios y casos de uso.
Interoperabilidad Transfronteriza	—	Siguiendo estándares internacionales de código abierto y utilizando registros de confianza accesibles, se fomenta la interoperabilidad transfronteriza. Esto promueve un ecosistema digital unificado donde las identidades digitales se pueden usar entre fronteras con reconocimiento y validación consistentes. Sin embargo, se necesita colaboración para desarrollar, mantener y usar registros de confianza interoperables.
Activos Tokenizados	✗	Las implementaciones de billeteras digitales en la UE y EE. UU. no incluyen funcionalidades para interactuar con activos digitales. Esto limita el uso de estas billeteras en el emergente panorama de las finanzas digitales y la tokenización, aunque iteraciones futuras podrían integrar esta capacidad.

5.3. eWallets 3.0 como billeteras digitales universales

Las iniciativas de eWallets 2.0 están destinadas a revolucionar la gestión de identidad a través de credenciales reutilizables que mejoran la seguridad y la escalabilidad. Este enfoque de próxima generación marca un paso significativo hacia la gestión de identidades digitales. No obstante, aún enfrenta incertidumbre en torno a la interoperabilidad transfronteriza y la integración fluida con activos tokenizados. Estas cuestiones deberán abordarse para garantizar que una próxima generación de billeteras digitales, las eWallets 3.0, pueda operar de manera eficiente a través de las fronteras nacionales y sea compatible con las finanzas digitales tokenizadas.

La interoperabilidad transfronteriza en la verificación de datos requiere un marco robusto donde todas las partes involucradas puedan confiar y acceder a registros de confianza comunes. En este modelo, los datos de identidad individuales se almacenan de forma segura en billeteras digitales y las pruebas verificables de los datos se mantienen y son accesibles en estos registros de confianza. Los registros de confianza, ya sean centralizados o descentralizados, garantizan que las billeteras digitales puedan proporcionar procesos de verificación confiables y universalmente aceptados, mejorando la utilidad y el alcance de las identidades digitales. Desarrollar una infraestructura técnica segura y accesible que respalde estos registros de confianza es fundamental.

Con respecto a la tokenización, las iniciativas de eWallets 2.0 no han integrado la identidad digital con funciones que permitan transacciones en

activos digitales. A medida que los mercados financieros y otros ecosistemas digitales se orientan cada vez más hacia la tokenización, existirá una mayor necesidad de que las billeteras digitales soporten un amplio espectro de activos digitales, desde criptomonedas y *stablecoins* hasta monedas digitales de bancos centrales (CBDC) y activos tokenizados del mundo real.

Las futuras iteraciones de eWallets probablemente servirán no solo como plataformas de verificación de identidad, sino también como interfaces integrales para la gestión y transacción en una amplia gama de activos digitales. Esta evolución impulsará soluciones de identidad digital consistentes con la próxima ola de innovación financiera y conducirá a la creación de eWallets 3.0 o, de manera equivalente, a las billeteras digitales universales.

Vale la pena destacar una vez más la importancia de los Puntos de Verificación (PoV). Los PoVs serán esenciales como endpoints que permiten a las organizaciones solicitar una autenticación digital y/o pago desde una billetera digital universal. Surgirá una industria completamente nueva para el desarrollo de soluciones de verificación que permitan crear reglas personalizadas para PoVs. Veremos PoVs en casi todos los sitios web y en cada pasarela de pago.



6. Blerify habilita billeteras digitales universales



Blerify sigue el modelo de identidad digital de la Unión Europea, alineándose con los marcos emergentes en Europa, Estados Unidos y Canadá para facilitar el desarrollo de soluciones de identidad interoperables en los sectores público y privado. Nuestra tecnología está meticulosamente diseñada para cumplir con estas normas internacionales para garantizar que la plataforma Blerify pueda interactuar sin problemas con diversos sistemas de identidad que mejoran la conectividad global y la flexibilidad operativa.

Además, Blerify va más allá de lo que exigen las billeteras digitales reguladas por el DAS2, ya que aborda varias de las limitaciones de estas billeteras, en particular las relacionadas con la interoperabilidad transfronteriza y la integración con activos tokenizados. En cuanto a la interoperabilidad transfronteriza, la tecnología Blerify incorpora capacidades avanzadas que se integran con registros de confianza centralizados y descentralizados para garantizar que las credenciales y las verificaciones de identidad sean reconocidas y verificables en diferentes países y sistemas. En cuanto a los activos tokenizados, la billetera digital de Blerify permite interacciones digitales seguras en transacciones y pagos tokenizados. Blerify es un innovador de eWallet 3.0 y permite una primera generación de billeteras digitales universales que están preparados para traer un cambio profundo en la forma en que realizamos transacciones en línea.

Blerify está especialmente preparado para servir tanto al sector público como al privado, ofreciendo soluciones a medida que abordan las necesidades específicas de cada ámbito. Para los organismos públicos, nuestra plataforma apoya el despliegue de identidades digitales y servicios de gobernanza electrónica, mejorando la participación ciudadana y la prestación de servicios. Para las empresas privadas, Blerify ofrece interfaces para aprovechar la billetera digital universal como nuevo canal para los usuarios finales. Esta adaptabilidad garantiza que, independientemente del sector, Blerify proporcione una solución que no sólo satisfaga las de-

mandas actuales, sino que también sea escalable y con visión de futuro, preparada para evolucionar con el cambiante panorama de la identidad digital y los servicios financieros. Esto se analiza con más detalle en el apéndice de este informe técnico, que describe los numerosos casos de uso que dependen de una billetera digital universal como la de Blerify.

6.1. Normas abiertas para la interoperabilidad universal

Nuestro enfoque en las soluciones de pago e identidad digital basadas en billeteras tiene como premisa la adopción y aplicación de normas abiertas, que garantizan la interoperabilidad, la seguridad y la escalabilidad en diversas plataformas y servicios a escala internacional. Seguimos la arquitectura de billeteras EUDI propuesta por la Unión Europea, así como normas ampliamente adoptadas para pagos móviles:

- **OpenID para credenciales verificables (OpenID4VC) y OpenID para presentaciones verificables (OpenID4VP):** Estos protocolos son fundamentales para hacer posible una verificación de identidad segura y que preserve la privacidad en diferentes plataformas. OpenID4VC permite la emisión y verificación de credenciales verificables, garantizando presentaciones de identidad digital fiables y a prueba de manipulaciones. OpenID4VP complementa esto permitiendo la presentación de credenciales de manera que mantenga la privacidad del usuario, garantizando que sólo se comparten los datos necesarios durante los procesos de autenticación.
- **Credenciales verificables del W3C:** El estándar *W3C Verifiable Credentials* proporciona un marco flexible y seguro para representar e intercambiar información de identidad. Este modelo promueve la creación de cre-

denciales digitales criptográficamente seguras, verificables y fácilmente compartibles entre plataformas. Al adherirse a esta norma, las soluciones de identidad digital son interoperables y están preparadas para el futuro, en consonancia con las mejores prácticas internacionales.

- **Identificadores descentralizados (DID) del W3C:** Los DID son un componente clave de un marco de identidad que ofrece un enfoque descentralizado de la gestión de identidades. A diferencia de los identificadores tradicionales ligados a entidades centralizadas, los DID permiten a individuos y organizaciones gestionar sus propios identificadores sin depender de un registro central. Esto mejora la privacidad, la seguridad y el control del usuario, en consonancia con los objetivos más amplios de los ecosistemas de identidad descentralizados.
- **Identificador de Personas Jurídicas (LEI):** El LEI es una norma reconocida internacionalmente para identificar a las personas jurídicas que participan en transacciones financieras. Los LEI garantizan que las identidades de las organizaciones estén representadas de forma única y precisa, lo que facilita el cumplimiento de los requisitos normativos globales y mejora la trazabilidad de las actividades financieras.
- **ISO/IEC 18013-5 Norma para licencias de conducir móviles (mDL):** mDL especifica cómo la información de identificación personal puede almacenarse de forma segura en dispositivos móviles y compartirse electrónicamente. Esta norma incluye protocolos para la protección de la privacidad, el control por parte del titular de la licencia y la interoperabilidad entre distintas jurisdicciones y tecnologías.
- **Passkeys:** Las Passkeys representan una evolución en la autenticación de usuarios, sustituyendo las contraseñas tradicionales por un método más seguro y fácil de usar. Aprovechan la criptografía de clave pública para autenticar a los usuarios sin necesidad de credenciales basadas en contraseñas, lo que reduce significativamente el riesgo de phishing y otras amenazas relacionadas con las contraseñas.
- **Tokens Web JSON (JWT):** JWT es un estándar abierto ampliamente utilizado para transmitir información de forma segura entre las partes como un objeto JSON. Se utiliza para el intercambio seguro de reclamaciones entre las partes, desempeñando un papel crucial en los procesos de autenticación y autorización dentro de los ecosistemas digitales.
- **Representación Concisa de Objetos Binarios (CBOR):** CBOR es un formato de datos optimizado para códigos y mensajes de pequeño tamaño, ideal para su uso en entornos con restricciones como los dispositivos IoT. Su eficiencia y compacidad lo convierten en una opción adecuada para codificar datos en sistemas de pago e identidad digital en los que el rendimiento es fundamental.
- **Normas NFC (Near Field Communication):** Las normas NFC, en particular las definidas por ISO/IEC 14443 e ISO/IEC 18092, son esenciales para permitir los pagos sin contacto a través de billeteras móviles. Estas normas garantizan una comunicación segura entre la billetera y los terminales de pago.
- **ISO 12812:** Norma para pagos por móvil que incluye los requisitos técnicos, operativos y de seguridad. Abarca las aplicaciones de pago por móvil, garantizando que cumplen criterios específicos de seguridad de las transacciones, protección de datos y autenticación de usuarios.
- **PSD2 (Directiva de Servicios de Pago 2):** Marco normativo de la Unión Europea que impone la autenticación fuerte del cliente (SCA) y estándares bancarios abiertos. La PSD2 afecta a las billeteras de pago al exigirles que admitan API abiertas, lo que permite compartir datos de forma segura con terceros proveedores y bancos.

- **Estándares ERC:** Al ser compatibles con los estándares ERC, las billeteras pueden integrarse a la perfección con el ecosistema de Ethereum, lo que permite a los usuarios interactuar con una amplia gama de activos digitales más allá de las monedas tradicionales. Permiten el uso de contratos inteligentes para automatizar procesos, reducir el fraude y mejorar la seguridad.

Al aprovechar estos estándares abiertos, Blerify crea una base sólida, flexible y segura para las soluciones de pago e identidad digital. Desde 2017, los miembros del equipo de Blerify han contribuido a los mayores grupos de trabajo involucrados en el desarrollo de estos estándares, incluyendo ISO, ITU, W3C, DIF, Linux Foundation, TrustOverIP, Open Wallet Foundation y WEF.

6.2. Identidad digital

Para hacer posible un mundo digital verificable, seguro y que preserve la privacidad, Blerify proporciona un modelo de identificación avanzado para individuos y un modelo de identificación para organizaciones.

6.2.1. Modelo de identificación de las personas

6.2.1.1. Credenciales verificables reutilizables

Nuestro planteamiento reconoce que las identidades digitales son dinámicas, definidas por atributos que varían en función de los distintos contextos, desde las plataformas de medios sociales hasta las redes profesionales. Cada contexto puede requerir la divulgación de atributos de identidad específicos, como el lugar de nacimiento, los registros financieros o las cualificaciones profesionales. La capacidad de controlar la divulgación de estos atributos es primordial, ya que incide directamente en la seguridad y la privacidad de la información personal.

Para solucionarlo, nuestro modelo aprovecha el marco de credenciales verificables del W3C, que permite a las personas gestionar y presentar sus credenciales directamente, sin necesidad de un proceso de verificación intermediario. Al poseer y gestionar sus credenciales, los usuarios pueden decidir cuándo, cómo y a quién revelar su información de identidad, incluidas las Pruebas de Conocimiento Cero (ZKP por su nombre en inglés), agilizando el proceso de autenticación y garantizando que se ajusta a sus preferencias de privacidad y seguridad. Este marco reconoce tres funciones:

- **Los emisores** son entidades que crean y expiden credenciales digitales a las personas. Estas credenciales contienen datos de identidad específicos relevantes para diferentes contextos.
- **Los titulares** de las billeteras poseen y controlan estas credenciales, decidiendo cuándo y dónde presentarlas.
- **Los proveedores** de servicio o verificadores son entidades que verifican la identidad (o los atributos) del titular de la billetera y, por tanto, exigen una prueba, que suele proporcionarse mediante la presentación de credenciales digitales.

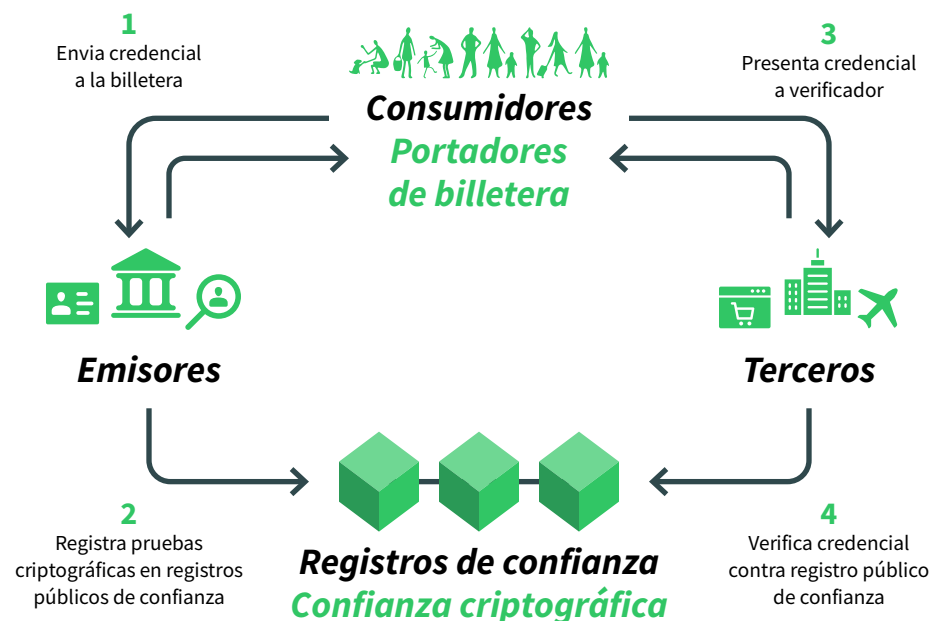
Las credenciales se estructuran como archivos digitales que contienen datos semiestructurados, formateados como pares campo-valor (por ejemplo, nombre=Rocío). Al aplicar este formato, las credenciales son tanto legibles por humanos como por máquinas, lo que facilita su uso en diversas plataformas y servicios. La billetera digital Blerify traduce estas credenciales a formatos fáciles de usar, como tarjetas digitales o PDF, y puede adaptar la presentación a varios idiomas, mejorando la accesibilidad y la comprensión. Esta capacidad garantiza que los usuarios puedan gestionar eficazmente sus identidades digitales de forma segura, eficiente y adaptada a sus necesidades.

Blerify proporciona una plataforma integral que permite a emisores, titulares y verificadores interactuar con datos en forma de credenciales verificables, con el usuario y la billetera digital como núcleo. Estas credenciales están firmadas digitalmente por la organización que las emite y selladas con fecha y hora en un registro de confianza accesible para que puedan verificarse fácilmente. Y, en caso de que la credencial ya no sea válida, el emisor puede modificar el estado de la credencial en el registro de confianza a "revocada" en cualquier momento después de su emisión. El proceso más básico puede desglosarse en 4 pasos que se presentan en la Figura 3.

Este enfoque presenta múltiples ventajas, como la interoperabilidad con el sector privado, la seguridad y la escalabilidad (que se identificaron como puntos débiles en las eWallets 1.0 y 2.0).

- **Interoperabilidad con los sectores público y privado:** Los gobiernos y las entidades del sector privado pueden emitir y verificar fácilmente credenciales digitales utilizando bibliotecas de código abierto y API proporcionadas por los proveedores de billeteras. Se convierten en emisores utilizando la plataforma Blerify para enviar credenciales digitales a las billeteras digitales universales. De este modo, la billetera se convierte en un canal centrado en el usuario para que las organizaciones interactúen con las personas y verifiquen su información de identidad sin tener que depender de terceros costosos e incómodos.
- **Seguridad:** Cuando se requiere verificación, las personas utilizan sus billeteras digitales para presentar sus credenciales digitales a terceros a través de canales cifrados. A continuación, los verificadores confirman la autenticidad de estas credenciales comprobando las marcas de tiempo criptográficas, las firmas del emisor y el estado de revocación en un registro de confianza accesible. Este enfoque reduce significativamente los posibles puntos de fallo únicos en las bases de datos de los emisores, limitando su exposición y mejorando la seguridad general.

Figura 3. Three-party framework for user-centric digital interactions describing the four steps for the issuance, presentation, and verification of digital credentials.



- **Escalabilidad:** El marco de seguridad apoya intrínsecamente la escalabilidad de nuestro sistema. Los modelos tradicionales, en los que miles de entidades emisoras deben integrarse directamente con un número igual de entidades verificadoras, no son sostenibles debido a la complejidad y las limitaciones de recursos. En cambio, nuestro modelo emplea un registro de confianza accesible al que pueden acceder todas las partes. Esta configuración permite la verificación escalable de credenciales sin necesidad de integraciones directas y engorrosas entre cada emisor y verificador. Al agilizar el acceso a las herramientas de verificación y descentralizar la emisión y el almacenamiento de credenciales, nuestro sistema se adapta eficientemente a un volumen creciente de transacciones y usuarios.

- **Interoperabilidad transfronteriza:** El uso de registros de confianza descentralizados permite a las instituciones privadas y públicas emitir, registrar y verificar pruebas criptográficas de datos de forma segura y universalmente accesible. Este método de descentralización supera las limitaciones de los sistemas centralizados tradicionales al permitir la interoperabilidad transfronteriza, en la que las credenciales y los datos pueden reconocerse y verificarse en distintas jurisdicciones y plataformas. Al crear un método de verificación estandarizado y a prueba de manipulaciones, Blerify garantiza que los datos sean fiables y aceptados en todo el mundo, fomentando un ecosistema interconectado que se adapta a la evolución de las necesidades de identidad digital y credenciales.

Figura 4. Ejemplo de credencial verificable tipo W3C en formato JSON.

```
// Example of data.json file
[
  {
    "id": 1,
    "firstName": "Thomas",
    "lastName": "Bækker",
    "address": {
      "streetName": "Tornelsevej",
      "streetNumber": "10",
      "city": "Solrød Strand"
    },
    "emergencyPhoneNumbers": ["+4530303030", "+4510203040"]
  },
  {
    "id": 2,
    "firstName": "Niels",
    "lastName": "Bohr",
    "address": {
      "streetName": "Flemsevej",
      "streetNumber": "31A",
      "city": "København"
    },
    "emergencyPhoneNumbers": []
  }
]
```

Figura 5. Imágenes de Billetera Digital Blerify.



6.2.1.2. Identificadores digitales

Como se ha comentado anteriormente, las credenciales contienen datos verificables estructurados en campos y valores. Para vincular de forma segura estas credenciales a los individuos y a sus billeteras digitales, es esencial incorporar pares de claves. Un par de claves se compone de una clave pública y una clave privada. Cuando una credencial está asociada a una clave pública, puede verificarse solicitando una firma utilizando la clave privada correspondiente, que el propietario legítimo almacena en su billetera digital.

Esencialmente, la presencia de la clave pública dentro de la credencial, junto con la clave privada necesaria para la firma, crea un vínculo seguro entre la credencial, su legítimo propietario y su billetera. Este mecanismo no sólo mejora la seguridad, sino que también garantiza que las credenciales sólo puedan ser utilizadas por sus legítimos titulares, evitando así el uso fraudulento.

Estas claves públicas sirven como identificadores que vinculan criptográficamente la credencial al individuo. Sin embargo, confiar únicamente en las claves públicas como identificadores es problemático. Las claves públicas son fijas y no pueden cambiarse fácilmente si se ponen en peligro, lo que hace que el sistema sea menos flexible y potencialmente menos seguro. Además, las claves públicas utilizadas en diferentes contextos pueden a veces revelar información personal identificable (IPI) no deseada, lo que plantea problemas de privacidad.

Un enfoque más sólido consiste en utilizar “identificadores paraguas” que puedan gestionar varios pares de claves bajo una misma identidad. Así, mientras que los identificadores nunca cambian, los pares de claves pueden rotarse o sustituirse según sea necesario sin interrumpir el vínculo entre la credencial y el individuo. Y, al utilizar un identificador paraguas, el

sistema puede seguir asociando de forma segura las credenciales con sus legítimos propietarios, al tiempo que ofrece una mayor protección de la privacidad al minimizar la exposición de la IPI. Este método garantiza una forma más flexible, segura y respetuosa con la privacidad de gestionar las credenciales digitales.

La nueva generación de credenciales digitales que representan certificados de salud, registros educativos, identificaciones gubernamentales, registros financieros y registros de empleo, entre otros, exige un mayor nivel de flexibilidad y seguridad en la gestión de identificadores y claves asociadas. Los identificadores y las credenciales verificables deben seguir siendo válidos a medida que las claves privadas asociadas a ellos se rotan o sustituyen.

Blerify aplica nuevas tecnologías para los identificadores digitales, incluidos los Identificadores Descentralizados (DID) y los Identificadores de Personas Jurídicas (LEI). Un DID es un identificador asociado a un documento DID que contiene las claves públicas, los protocolos de autenticación y los endpoints de servicio necesarios para interactuar con el sujeto DID. Este documento DID puede actualizarse para rotar claves o cambiar métodos de autenticación sin cambiar el propio DID. Los documentos DID pueden mantenerse en diferentes tipos de registros de confianza.

En caso de que una clave se vea comprometida, el documento DID puede actualizarse rápidamente con un nuevo par de claves, garantizando la continuidad de la validez del identificador sin tener que volver a emitir la credencial completa. Del mismo modo, en caso de pérdida de la clave, los mecanismos de recuperación pueden predefinirse en el marco del DID, lo que permite al propietario legítimo recuperar el control sobre su identificador.

Este proceso es totalmente transparente para las personas, que nunca necesitan involucrarse a un nivel técnico tan profundo. La billetera digital Blerify puede realizar todas las acciones necesarias relacionadas con las

Figura 6. Ejemplo de Documento DID alineado con W3C.

```
Minimal self-managed DID Document
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

actividades de gestión de identificadores que maximizan la privacidad y la seguridad. Blerify está diseñado para ser interoperable con múltiples métodos DID, y también ha desarrollado su propia implementación de código abierto del método DID "did:blr" que es ideal para asegurar la privacidad de los individuos. Este enfoque avanzado de los identificadores digitales, facilitado por la vinculación criptográfica a través de pares de claves y mejorado por la flexibilidad de normas como los DID y los IPJ, representa una evolución significativa en la gestión de la identidad digital. Proporciona a las personas y entidades un mayor control, seguridad y resistencia en sus interacciones digitales, garantizando que sus credenciales e identificadores asociados puedan adaptarse a las cambiantes necesidades de seguridad y a los avances tecnológicos.

6.2.1.3. Seguridad contra suplantaciones de Deepfakes de IA

La verificación biométrica, como las huellas dactilares, el reconocimiento facial y el escaneo de iris, se ha considerado tradicionalmente como un método sólido para verificar la identidad de una persona. Sin embargo, con la llegada de las tecnologías avanzadas de IA, incluidas las IA deepfake, esta forma de verificación se ha vuelto cada vez más vulnerable al fraude. Las IA de imitación deepfake pueden generar ahora datos biométricos sintéticos muy realistas, que tienen el potencial de eludir los sistemas biométricos tradicionales. Esto ha creado una gran preocupación sobre la verificación biométrica para la verificación de la identidad.

Por otro lado, una persona que presenta múltiples credenciales y documentos verificables de diferentes fuentes de confianza ofrece un método más seguro para la verificación de la identidad. Estas credenciales, cuando se vinculan criptográficamente a la identidad digital del individuo y se almacenan en su billetera digital universal, proporcionan múltiples capas de prueba que, en conjunto, hacen mucho más difícil que esa persona pueda ser suplantada maliciosamente. Dado que cada credencial y documento puede verificarse de forma independiente en un registro de confianza, el sistema en su conjunto es más resistente al fraude y a los ataques de falsificación.

Este enfoque es el núcleo de un nuevo campo de estudio que explora el concepto de *personhood credential*. Investigadores y tecnólogos están trabajando en sistemas en los que la identidad única de un individuo se demuestra no a través de un único dato biométrico, sino mediante una combinación de credenciales verificables [20]. Estas credenciales pueden incluir identificaciones emitidas por el gobierno, certificados educativos, credenciales laborales y otros documentos emitidos por entidades de confianza. Al agregar estas diversas fuentes de prueba, el sistema garantiza

que el individuo es realmente quien dice ser, sin depender de un único factor biométrico potencialmente vulnerable.

Las billeteras digitales universales son parte integrante de esta solución. Sirven como contenedores seguros para estas diversas credenciales, permitiendo a los individuos gestionar y presentar sus credenciales de una manera que es a la vez conveniente y segura. Dado que cada credencial está vinculada criptográficamente a la identidad digital del individuo dentro de su billetera, el sistema proporciona una seguridad sólida al tiempo que protege la privacidad. El individuo conserva el control sobre su identidad y puede elegir qué credenciales compartir, dependiendo del contexto, al tiempo que garantiza que cada credencial es verificable de forma independiente.

6.2.1.4. Pruebas de conocimiento cero

Las pruebas de conocimiento cero (en inglés *Zero-Knowledge Proofs* o ZKP) son un método criptográfico que permite a una parte demostrar a otra (el verificador) que una afirmación dada es verdadera, sin revelar ninguna información más allá de la validez de la propia afirmación. Esta tecnología tiene importantes implicaciones para la privacidad y la seguridad en las interacciones digitales, lo que la hace especialmente valiosa en el contexto de la gestión y verificación de credenciales digitales. Por ejemplo, una ZKP podría permitir a alguien demostrar que supera la edad legal para consumir alcohol o que tiene derecho a acceder a contenidos para adultos sin revelar su fecha exacta de nacimiento. Así, la ZKP es clave para minimizar la cantidad de datos personales expuestos durante las transacciones digitales, lo que mejora la privacidad del usuario.

Nuestro enfoque de utilizar credenciales verificables es especialmente adecuado para la integración con ZKP debido a su estructura criptográfica inherente. Cuando estas credenciales se utilizan junto con la función ZKP,

el individuo que recibe la credencial puede crear divulgaciones selectivas de dicha credencial a terceros en las que sólo se comparten campos y valores seleccionados de las credenciales. Las ZKP pueden entonces aplicarse a estas credenciales para permitir a los individuos demostrar la validez de las afirmaciones a un verificador sin revelar ninguna información adicional más allá de lo necesario. Este proceso aprovecha la fuerza criptográfica tanto de la firma digital como de la prueba de conocimiento cero, lo que la convierte en una combinación ideal para procesos de verificación seguros y privados en los que es crucial revelar la mínima información personal.

6.2.2. Modelo de identificación para organizaciones

6.2.2.1. Una revisión de la actual raíz de confianza de las interacciones web basadas en navegadores

El ecosistema web actual verifica las identidades organizativas predominantemente a través de navegadores que utilizan certificados electrónicos X.509. Estos certificados son un formato estándar para certificados de clave pública, emitidos por Autoridades de Certificación (CA, por su nombre en inglés), que son entidades de confianza que certifican la autenticidad del titular del certificado. Cuando un usuario accede a un sitio web seguro, el navegador comprueba el certificado X.509 del sitio web para asegurarse de que es válido y ha sido emitido por una autoridad de confianza. Este proceso es crucial para establecer comunicaciones seguras y cifradas a través de Internet.

Todos estos elementos son críticos para habilitar la Raíz de Confianza (RoT) necesaria para la autenticación segura y la comunicación entre organizaciones. Comprender esta RoT es esencial para analizar cómo puede construirse una nueva RoT para la nueva generación de interacciones digitales en la que las billeteras digitales sustituyen a los navegadores como interfaces digitales para las interacciones digitales, y los registros de confianza a las CA.

Como ya se ha mencionado, la actual RoT para identidades organizativas en Internet se basa en la fiabilidad de las CA y en la fiabilidad del proceso de validación de certificados implementado por los navegadores. La emisión y verificación de identidades organizativas funcionan de la siguiente manera:

Emisión de identidad organizativa

- **Solicitud de certificado:** Las organizaciones que desean establecer su verificabilidad en Internet inician el proceso solicitando a una Autoridad de Certificación (CA) que les expida un certificado X.509.
- **Verificación por parte de las CA:** La CA verifica la identidad de la organización exigiendo una prueba de control del dominio y revisando documentos fundacionales como los documentos de constitución. Este paso garantiza la legitimidad de la organización que solicita el certificado.
- **Emisión del certificado:** Una vez verificado, la CA emite un certificado X.509 para la organización. Este certificado incluye la clave pública de la organización y otros datos identificativos.
- **Resolución y revocación de certificados:** Los certificados X.509 son soportados por navegadores que pueden autenticarlos contra Autoridades Certificadoras (CAs) de confianza incluidas en la lista inherente de CAs de confianza del navegador. Los estados de revocación se comprueban con listas de revocación de certificados (CRL) o en tiempo real a través del protocolo de estado de certificados en línea (OCSP).

Verificación de la identidad de la organización

- **Acceso a sitios web:** Cuando una persona intenta acceder a un sitio web, el navegador recupera el certificado X.509 del sitio para iniciar el proceso de verificación.

- **Resolución de certificados:** El navegador comprueba si el certificado está emitido por una CA de confianza incluida en la raíz de confianza (RoT) del navegador.
- **Comprobación de revocación:** El navegador también verifica el estado de revocación del certificado para confirmar que no ha sido revocado o reportado como comprometido. Esto se hace normalmente utilizando CRL u OCSP. El navegador se asegura de que el certificado es actual y válido antes de establecer una conexión segura con el sitio web.

6.2.2.1. Solución pionera de Blerify para un modelo descentralizado de raíz de confianza (DRoT) para las interacciones web basadas en billeteras

Comprender la dinámica y la estructura de la RoT (cadena de confianza) que se utiliza actualmente para proteger los sitios web resulta útil cuando navegamos hacia un nuevo ecosistema basado en billeteras que incluye credenciales digitales, activos digitales y toda una nueva generación de productos y servicios basados en billeteras. Para acomodar y asegurar estas conexiones e interacciones, es necesario reconstruir la actual RoT a lo largo de las tres dimensiones descritas a continuación:

- **Conexiones seguras Billetera-organización:** Las billeteras digitales deben ser capaces de resolver y verificar la identidad de una organización con una RoT de confianza. Esto permite a los titulares de las billeteras verificar la identidad de las organizaciones con las que se conectan desde sus billeteras y decidir si dan su consentimiento a las conexiones. Esto garantiza que las interacciones con partes de confianza sean seguras y fiables, y protege contra posibles amenazas y violaciones de la seguridad.
- **Verificación de credenciales de emisores:** Cuando los verificadores pretenden validar datos presentados en forma de credencial verificable,

deben poder confirmar el emisor de la credencial con una RoT. Este paso es fundamental para determinar la fiabilidad de los certificados vinculados a las credenciales, ya sea un documento de identidad expedido por una organización profesional o un diploma expedido por una universidad. Este proceso garantiza que las credenciales no sólo son auténticas, sino que además están respaldadas por entidades legítimas y reconocidas.

- **Verificación de la procedencia de los activos digitales:** Tanto los particulares como las organizaciones necesitan verificar la procedencia de los activos digitales, así como la identidad de sus emisores. Este proceso de verificación ayuda a confirmar la autenticidad y legitimidad de los activos digitales. Al permitir a las entidades emisoras establecer una cadena de propiedad clara y rastreable, es posible verificar que los activos son auténticos.

Blerify ha desarrollado una solución pionera para una RoT Descentralizada (DRoT) basada en una Infraestructura de Clave Pública Descentralizada (DPKI) que aprovecha lo mejor de las RoT tradicionales basadas en navegadores y también aborda las necesidades emergentes que demandan las billeteras digitales, las credenciales y los activos. Nuestra solución emplea un registro de confianza descentralizado e identificadores flexibles, siguiendo un enfoque accesible, seguro e interoperable.

Hemos desarrollado cuatro contratos inteligentes que facilitan el despliegue de una DRoT en un registro de confianza descentralizado. Esto permite la verificación de las identidades de las organizaciones con el fin de establecer conexiones seguras entre las billeteras y las organizaciones, la verificación de los emisores de credenciales y la validación de la procedencia de los activos. Estos contratos inteligentes pueden describirse como sigue:

1. **Registro de identificadores:** Este contrato inteligente permite a cualquier organización registrar un identificador de organización

autogenerado junto con las claves públicas y los endpoints asociados (por ejemplo, dominio, URL, correo electrónico). Las organizaciones pueden mantener el mismo identificador mientras añaden, revocan o actualizan las claves públicas o endpoints asociados, según sea necesario. En caso de compromiso, la organización puede indicar la fecha a partir de la cual se comprometió la clave o el endpoint, permitiendo a otros resolver y verificar esta información cuando sea necesario. Dado que este contrato inteligente es de acceso público en un registro de confianza descentralizado, como una red blockchain, cualquiera puede verificar el identificador de una organización y las claves asociadas.

2. **Controlador de identidad de una organización:** Este contrato inteligente proporciona a las organizaciones una capa adicional de gestión de identidades a través de la delegación. Las organizaciones pueden establecer identificadores delegados típicamente asociados con empleados, subentidades o afiliados autorizados para representar a la organización en interacciones digitales específicas (por ejemplo, emitir una credencial específica). Aquí se aplica la misma flexibilidad para añadir, revocar y actualizar claves públicas y endpoints.

3. **Directorio de identificadores públicos:** Aunque los dos primeros contratos inteligentes permiten a las organizaciones gestionar sus identificadores, claves públicas y endpoints, sigue siendo necesaria una Autoridad de Certificación (AC) para verificar y certificar una organización y sus identificadores, garantizando que terceros puedan confiar en la identidad de la organización. Este tercer contrato inteligente, desplegado y mantenido por una CA, sirve a este propósito indexando los identificadores de la organización con metadatos como nombre, dominio, dirección legal y correo electrónico.

4. **Listas de confianza:** El cuarto contrato inteligente está diseñado para establecer marcos de confianza para certificar organizaciones con fines

específicos relacionados con la emisión de credenciales y activos. Por ejemplo, las instituciones educativas podrían formar parte de un marco de confianza para el reconocimiento mutuo de diplomas, o las entidades sanitarias podrían formar parte de un marco de confianza con el fin de emitir resultados de pruebas específicas. Este contrato inteligente es operado por una organización de confianza que mantiene una lista de organizaciones certificadas y sus respectivos propósitos.

6.2.3. Resistencia cuántica

La llegada de la computación cuántica representa tanto un salto innovador como una importante amenaza para las medidas de seguridad criptográficas que sustentan gran parte de la infraestructura digital actual. La capacidad de procesamiento de los ordenadores cuánticos romperá la mayoría de los algoritmos criptográficos que se utilizan actualmente para proteger desde las transacciones financieras hasta las comunicaciones personales, según las mayores agencias tecnológicas del mundo, entre ellas el NIST, NSA, y ETSI.

Uno de los usos potenciales más discutidos de la computación cuántica es la ruptura de algoritmos criptográficos. Muchos de los métodos de cifrado actuales, como RSA y ECC (criptografía de curva elíptica), se utilizan hoy en día para cifrar y firmar todas las comunicaciones a través de Internet. Por tanto, las soluciones actuales y futuras para la identidad digital exigen enfoques resistentes a la tecnología cuántica que impidan hackeos masivos.

En respuesta a estas amenazas potenciales, ha surgido el campo de la criptografía post-cuántica, centrado en el desarrollo de sistemas criptográficos que sean seguros tanto contra ordenadores cuánticos como clásicos. Los algoritmos criptográficos post-cuánticos están diseñados para funcionar en ordenadores tradicionales, pero son resistentes a los ataques de los ordenadores cuánticos.

Los miembros del equipo fundador de Blerify han sido reconocidos como pioneros en el desarrollo de soluciones, herramientas y marcos resistentes a la cuántica. En concreto, desarrollaron la primera implementación de una red blockchain resistente a la cuántica, como se señala en un artículo sobre el tema publicado por la revista Scientific Reports de Nature). [21] También contribuyeron como coautores a los Principios de Gobernanza de la Computación Cuántica desarrollados por el Foro Económico Mundial (WEF) [22].

Nuestra plataforma está diseñada para funcionar con la nueva generación de algoritmos criptográficos que actualmente está normalizando el NIST [23]. El uso de credenciales verificables y de un identificador digital, que constituyen el núcleo de nuestra infraestructura tecnológica, también es ideal para la criptografía resistente a la cuántica que ha pasado a formar parte de nuestra solución. [24]

6.3. Pagos digitales

6.3.1. Métodos de pago tradicionales

La billetera digital universal de Blerify integra a la perfección los métodos de pago tradicionales en su plataforma, garantizando a los usuarios una experiencia de gestión financiera completa. La billetera admite transacciones a través de tarjetas de crédito y débito estándar, sirviendo de puente entre los métodos bancarios convencionales y la comodidad digital moderna. Esta integración permite a los usuarios utilizar métodos de pago conocidos y disfrutar al mismo tiempo de las funcionalidades mejoradas de una billetera digital.

Para facilitar transacciones fluidas y seguras, Blerify utiliza tecnologías avanzadas como NFC (Near Field Communication), códigos QR y códigos

de barras. NFC permite la comunicación sin contacto entre la billetera y los terminales de pago, ofreciendo una forma rápida y segura de realizar transacciones con un simple toque. Los códigos QR y los códigos de barras proporcionan opciones versátiles para iniciar transacciones, permitiendo a los usuarios realizar pagos escaneando códigos que aparecen en dispositivos o materiales impresos. Este enfoque multi-tecnológico no sólo diversifica las opciones de pago, sino que también garantiza que las transacciones sean accesibles y cómodas, atendiendo a una amplia gama de preferencias y escenarios de usuario.

6.3.3. *Stablecoins*

La billetera Blerify incorpora *stablecoins* para satisfacer la creciente demanda de soluciones de pago globales eficientes y fiables. Las *stablecoins*, que suelen estar vinculadas a activos "estables" como monedas fiduciarias o materias primas, proporcionan la estabilidad de precios necesaria para las transacciones diarias, al tiempo que mantienen las ventajas de la tecnología de las divisas digitales. Esta integración permite a los usuarios de Blerify realizar pagos instantáneos sin la volatilidad asociada a las criptomonedas tradicionales.

El uso de *stablecoins* en las billeteras digitales universales mejora significativamente el proceso de pagos transfronterizos. Al eliminar los retrasos y las elevadas comisiones que suelen asociarse a los sistemas bancarios tradicionales, Blerify ofrece una solución más práctica para el comercio internacional, las remesas y los servicios financieros transfronterizos. Este enfoque racionalizado garantiza que las transacciones no sólo sean más rápidas, sino también más seguras, ya que la tecnología blockchain sustenta la integridad y la transparencia de cada transacción. De este modo, la billetera de Blerify permite algo más que el simple procesamiento de pagos para facilitar una red financiera global más conectada y accesible.

6.4.4. Formas alternativas de valor

La plataforma de Blerify es pionera en el uso de formas alternativas de valor -más allá del dinero digital tradicional- para pagos y transacciones. Este enfoque innovador incluye la integración de cupones, vales, puntos de fidelidad, millas aéreas y otras recompensas no monetarias, permitiendo que estos activos se utilicen sin problemas como medios de pago. Esta flexibilidad crea nuevas vías para las organizaciones que buscan atraer e incentivar a franjas enteras de clientes, ciudadanos, miembros y otros. También permite a los particulares aprovechar las recompensas acumuladas de forma práctica y beneficiosa, aumentando la utilidad y el atractivo de la plataforma Blerify.

Los vales digitales desempeñan un papel especialmente importante en la billetera Blerify. Estos vales actúan como fichas canjeables digitalmente que pueden utilizarse para agilizar la distribución de ayuda y los procesos de envío de remesas, entre otras cosas. En el contexto de la inclusión financiera, los vales digitales son una herramienta fundamental para prestar ayuda financiera a las poblaciones no bancarizadas, que a menudo carecen de acceso a los servicios bancarios convencionales. Por ejemplo, en situaciones de ayuda en caso de catástrofe o en programas de bienestar social, las autoridades y organizaciones podrán distribuir vales digitales directamente a través de la billetera Blerify, garantizando que la ayuda llegue a sus destinatarios de forma rápida y segura.

6.3.5. Criptomonedas

La comodidad y la facilidad de uso de las billeteras para criptomonedas serán primordiales a medida que las monedas digitales sigan integrándose en las prácticas financieras dominantes. La billetera digital universal de Blerify está diseñada teniendo en cuenta estas prioridades, garantizando que la gestión de criptodivisas no solo sea segura, sino también excepcionalmente fácil de usar.

Un elemento central de nuestra propuesta de valor es el innovador modelo de identidad de Blerify, que aprovecha las credenciales verificables para facilitar procesos sólidos de verificación de la identidad. Este modelo es ideal para procedimientos exhaustivos de Conozca a su Cliente (KYC) y Anti-Lavado de Dinero (AML). Al utilizar credenciales verificables, Blerify permite a los usuarios demostrar su identidad de forma segura y eficiente, sin la presentación repetitiva de documentos personales. Esto no sólo mejora la comodidad del usuario, sino que también reduce significativamente el potencial de fraude, garantizando que las organizaciones que confían en la plataforma Blerify se adhieren a los más altos estándares de cumplimiento normativo.

Además, anticipamos que cada vez más países implementarán la Regulación *Travel Rule* para transacciones en criptomonedas, y la normal probablemente se aplicará a billeteras no custodiadas como la de Blerify. La arquitectura de nuestra billetera está diseñada para gestionar de forma responsable el intercambio requerido de información transaccional, garantizando que todas las transferencias cumplan las normas reguladoras globales sin comprometer la privacidad del usuario.

6.3.6. Monedas digitales de bancos centrales (CBDC)

Nuestra billetera digital universal está estratégicamente posicionada para capitalizar la integración de las monedas digitales de los bancos centrales (CBDC, por sus siglas en inglés), diseñadas para salvar la brecha entre los sistemas financieros tradicionales y las modernas tecnologías financieras digitales. Las CBDC, emitidas y reguladas por los bancos centrales, ofrecen una alternativa digital a las monedas fiduciarias tradicionales, combinando la fiabilidad y la supervisión reguladora de los bancos centrales con la eficiencia y la innovación de la tecnología blockchain.

Esto es especialmente beneficioso para los pagos globales, en los que las CBDC pueden reducir significativamente los costes y complejidades

típicamente asociados al cambio de divisas y las transferencias transfronterizas de dinero. Al ofrecer soporte para las CBDC, Blerify no sólo mejora la utilidad de su plataforma para las transacciones cotidianas, sino que también se alinea con los futuros ecosistemas financieros que probablemente estarán dominados por monedas nativas digitales. Este enfoque con visión de futuro garantiza que los usuarios de Blerify tengan acceso a una herramienta completa, segura y eficiente para navegar por el cambiante panorama de las finanzas mundiales.

6.4. Integración con registros de confianza

Los registros de confianza centralizados y descentralizados desempeñan un papel fundamental en la gestión de identidades, credenciales y activos digitales, y cada uno cumple funciones específicas que satisfacen las diversas necesidades de los usuarios y las organizaciones dentro del ecosistema digital.

Los registros de confianza centralizados son cruciales para las organizaciones que requieren un acceso controlado a datos y registros confidenciales. Estos registros proporcionan un entorno seguro en el que las organizaciones pueden mantener registros privados con altos niveles de seguridad y privacidad. Al centralizar el almacenamiento y la gestión de los datos, estos registros garantizan que el acceso esté estrictamente regulado y que se mantenga la integridad de los datos. Esto es especialmente importante para las empresas e instituciones que necesitan salvaguardar información privada o cumplir estrictas normativas de protección de datos.

El uso de registros de confianza centralizados, aunque beneficioso para mantener el control sobre los datos sensibles, a menudo se enfrenta a importantes problemas de escalabilidad cuando se integra a través de API con

otras entidades. Estos sistemas pueden limitar la accesibilidad debido a su naturaleza cerrada, requiriendo integraciones específicas para cada nueva parte, lo que puede ser engorroso y consumir muchos recursos. Además, los registros centralizados son propensos a los ciberataques y las brechas, ya que presentan objetivos lucrativos para los piratas informáticos que buscan explotar puntos de fallo únicos. Esta vulnerabilidad no sólo pone en peligro la seguridad de los datos, sino también la integridad de todo el sistema, haciéndolo menos fiable para los usuarios que dependen de estos registros para realizar transacciones críticas y verificar su identidad. Estas limitaciones ponen de manifiesto la necesidad de soluciones más seguras y adaptables para gestionar las identidades y transacciones digitales.

Por otro lado, los registros de confianza descentralizados destacan por promover la accesibilidad y la interoperabilidad entre diversas plataformas y sistemas. A diferencia de los modelos centralizados, los registros descentralizados utilizan la tecnología blockchain o tecnologías similares para almacenar pruebas criptográficas de datos o transacciones. Este enfoque permite un registro transparente e inmutable al que se puede acceder públicamente sin necesidad de integración o interacción directa.

En el contexto de las credenciales digitales, los registros de confianza descentralizados permiten un enfoque centrado en el usuario en el que los emisores pueden registrar pruebas criptográficas de credenciales que los verificadores pueden verificar de forma independiente. Este modelo elimina la necesidad de comunicación directa entre el emisor y el verificador, fomentando un proceso de verificación más abierto y accesible. Admite situaciones en las que los usuarios necesitan demostrar sus cualificaciones o su identidad en múltiples plataformas sin tener que someterse repetidamente a procesos de verificación.

Para los activos y pagos digitales, los registros de confianza descentralizados facilitan la transferencia instantánea de valor. Esta capacidad es

transformadora para las transacciones financieras, especialmente en el comercio global y los intercambios entre pares. Al permitir la transferencia inmediata y segura de activos sin necesidad de intermediarios, los registros descentralizados reducen los tiempos de transacción, disminuyen los costes y mejoran la eficiencia general de las transacciones digitales.

Los registros de confianza descentralizados permiten a los emisores de credenciales digitales registrar pruebas criptográficas que pueden ser verificadas por otra parte sin interacción directa o integración con la otra parte. Este enfoque permite un nuevo proceso de verificación en el que los individuos, en lugar de terceros, están en el centro del proceso de verificación, recibiendo credenciales verificables de los emisores y presentándolas a los verificadores, maximizando la verificabilidad, la interoperabilidad, la escalabilidad y la privacidad.

La plataforma Blerify aborda de forma única los retos de integración de los registros de confianza centralizados y descentralizados, ofreciendo a las organizaciones una solución versátil y segura para integrarse con billeteras digitales universales. Al permitir que las organizaciones se conecten a registros de confianza descentralizados a través de API seguras, Blerify garantiza que las organizaciones puedan mantener el control sobre sus datos confidenciales al tiempo que se benefician de una mayor conectividad e interoperabilidad en sus registros de confianza centralizados. Esta integración permite flujos de datos fluidos entre diferentes sistemas, mejorando la eficiencia y escalabilidad de las operaciones. Blerify se dedica a facilitar las interacciones globales a través de billeteras digitales universales, garantizando que cada intercambio mantiene los más altos estándares de privacidad, seguridad y cumplimiento, al tiempo que mantiene la mejor experiencia de usuario. Este enfoque de doble registro no sólo mejora la eficiencia de las transacciones, sino que también amplía el acceso a los mercados de activos digitales, fomentando un entorno económico más inclusivo y fluido.

6.5. Ventajas de la infraestructura de billetera universal de Blerify

Eficacia y comodidad	✓	Igual que eWallets 2.0.
Accesibilidad	✓	Igual que eWallets 2.0.
Notificaciones	✓	Igual que eWallets 2.0.
Inclusión financiera	✓	Igual que eWallets 2.0.
Seguridad	✓	Igual que eWallets 2.0.
Escalabilidad	✓	Igual que eWallets 2.0.
Interoperabilidad transfronteriza	✓	Seguir normas internacionales de código abierto y utilizar registros de confianza accesibles permite la interoperabilidad transfronteriza. Esto crea un ecosistema digital unificado en el que las identidades digitales pueden utilizarse a través de las fronteras con una verificabilidad y aceptación coherentes.
Activos tokenizados	✓	La infraestructura de la billetera de identidad digital Blerify permite a los titulares de la billetera enviar y recibir activos digitales, incluidos tokens digitales. La combinación de credenciales de identidad con activos tokenizados permite un nuevo paradigma de transacciones y pagos digitales seguros, eficientes y verificables.

Apéndice

Casos de uso por industria

A.1 Identificación y servicios gubernamentales

Las billeteras digitales universales transformarán la forma en que los gobiernos interactúan con los ciudadanos al proporcionar mecanismos seguros y eficientes para la gestión de la identidad y la prestación de servicios. A continuación, se exponen varios casos clave de uso de la identificación y los servicios públicos facilitados por las billeteras digitales universales:

- **Emisión de DNI electrónicos con los máximos niveles de seguridad:** Las billeteras digitales universales pueden almacenar identificaciones electrónicas (eID) que cumplen los más altos niveles de seguridad según la normativa ISO, asegurando que son a prueba de manipulaciones y están vinculadas de forma segura a su legítimo propietario a través de métodos criptográficos avanzados. Estos eID pueden utilizarse para diversos fines de verificación, ofreciendo una alternativa digital fiable a los métodos tradicionales de identificación física.
- **Acceso a los servicios públicos:** Las billeteras digitales simplifican el proceso de acceso a los servicios públicos almacenando todas las credenciales necesarias en un solo lugar. Los ciudadanos pueden utilizar las identificaciones electrónicas almacenadas en sus billeteras para acceder a los portales de la Administración, solicitar permisos o

acceder a los servicios de salud pública. Este acceso simplificado no sólo mejora la experiencia del usuario, sino que también reduce la carga administrativa de los organismos públicos.

- **Monetización de los eID para la autenticación de alto nivel frente al sector privado:** La integración de los eID en las billeteras digitales permite procesos de autenticación de alto nivel, lo que los hace ideales para transacciones financieras sensibles. Los gobiernos pueden monetizar estos eID, en relación con la prestación de diversos servicios, como la banca, las solicitudes de crédito y otras interacciones financieras, aumentando la confianza y reduciendo el fraude. En la actualidad, sólo los proveedores de CSC son plenamente responsables de estos servicios y de su monetización.
- **Distribución de ayuda y transferencias condicionadas de efectivo:** Los gobiernos pueden utilizar billeteras digitales para distribuir ayuda directamente a las billeteras de los ciudadanos, garantizando que la ayuda llegue a los destinatarios previstos de forma rápida y segura. Estas billeteras también pueden facilitar las transferencias de efectivo condicionadas, en las que los fondos se liberan si el beneficiario cumple determinadas condiciones, como asistir a un chequeo médico o matricular a los niños en la escuela.

- **Votaciones:** Las billeteras digitales pueden revolucionar el proceso de votación al permitir mecanismos de voto en línea seguros y verificables. Los ciudadanos pueden emitir su voto a través de su billetera digital, donde su identidad se verifica con sus eID almacenados, garantizando un proceso de votación seguro y anónimo. Este método puede aumentar la participación al hacer el voto más accesible y mantener la integridad del proceso electoral.
- **Encuestas:** Los gobiernos pueden utilizar las billeteras digitales para realizar encuestas y recopilar datos directamente de los ciudadanos de forma seudónima. Al aprovechar los canales de comunicación seguros y verificados de las billeteras digitales, las autoridades pueden garantizar que los datos recopilados son fiables y que las respuestas proceden realmente de los electores.
- **Transporte público:** La integración de las billeteras digitales con los sistemas de transporte público permite una mejor experiencia de transporte. Los ciudadanos pueden utilizar sus billeteras digitales para acceder a las redes de transporte público, pagar tickets y gestionar sus créditos de viaje, reduciendo la necesidad de billetes o tarjetas físicas.
- **Facturas de servicios públicos, como la electricidad, el agua y el gas:** Los usuarios pueden recibir facturas digitales de electricidad, agua y gas, establecer pagos automáticos y recibir recordatorios puntuales, lo que garantiza que las facturas se pagan de forma eficiente y sin intervención manual. Además, estas billeteras pueden almacenar historiales detallados de transacciones para el seguimiento financiero y la elaboración de presupuestos. También facilitan la comunicación directa con el servicio de atención al cliente en caso de discrepancias o problemas con el servicio. Además, las empresas de servicios públicos podrían incentivar el uso de billeteras digitales ofreciendo descuentos o puntos de fidelidad, mejorando la satisfacción del cliente y fomentando los pagos puntuales. Esta

integración no sólo simplifica la gestión de las facturas, sino que también mejora la experiencia general del usuario con los servicios públicos.

- **Recompensas por prácticas sostenibles:** Las billeteras digitales universales también pueden aprovecharse para promover y recompensar comportamientos cívicos, como el reciclaje y la reducción de la huella de carbono. Mediante la integración de programas de recompensas medioambientales, las billeteras pueden incentivar a los usuarios a adoptar prácticas sostenibles ofreciéndoles fichas digitales o créditos por acciones como reciclar adecuadamente los residuos o elegir opciones de transporte alineadas con el medio ambiente. Estas recompensas pueden utilizarse dentro del sistema de billeteras para canjear beneficios como descuentos en el transporte público, impuestos más bajos o subvenciones a productos y servicios ecológicos.

Estos casos de uso ponen de relieve las muchas aplicaciones de las billeteras digitales universales para mejorar los servicios públicos y la participación ciudadana. Al proporcionar una plataforma segura, centralizada y fácil de usar, las billeteras digitales pueden desempeñar un papel fundamental en el futuro de la administración pública y los servicios comunitarios.

A.2. ONG

Las billeteras digitales universales pueden mejorar significativamente las operaciones de las organizaciones no gubernamentales (ONG) al agilizar procesos como la distribución de ayuda económica, la verificación de identidades y la gestión de credenciales profesionales. He aquí algunos casos de uso concretos:

- **Distribución de la ayuda:** Las ONG pueden utilizar billeteras digitales para distribuir ayuda financiera directamente a los beneficiarios de forma segura y eficiente. Mediante la transferencia de fondos a billeteras

digitales individuales, las ONG pueden garantizar que la ayuda llegue rápidamente a los destinatarios, reduciendo el riesgo de robo o mala gestión. Este método también permite a las ONG hacer un seguimiento y una auditoría de los fondos, lo que favorece la transparencia y la rendición de cuentas en los programas de ayuda. Además, las billeteras digitales pueden facilitar las transferencias de efectivo condicionadas, en las que los fondos se liberan cuando los beneficiarios cumplen determinadas condiciones, como asistir a programas educativos o revisiones médicas. Esta distribución digital de la ayuda no requiere que los beneficiarios tengan cuentas bancarias, que es uno de los mayores retos actuales.

- **Credenciales de identidad para poblaciones desplazadas:** Para las poblaciones desplazadas por conflictos o catástrofes naturales, establecer la identidad puede ser un gran reto. Las ONG pueden utilizar billeteras digitales para emitir credenciales de identidad digitales verificables que las personas puedan utilizar para acceder a servicios como la sanidad, la banca y la asistencia jurídica. Estas identificaciones digitales pueden ser reconocidas internacionalmente, ayudando a los refugiados y desplazados a establecer su identidad en nuevos países sin los habituales problemas burocráticos migratorios.
- **Certificados de competencias y registros profesionales verificables:** Las billeteras digitales pueden almacenar certificados de aptitudes y registros profesionales, lo que facilita a las personas mantener y compartir pruebas de sus cualificaciones. Las ONG que participan en programas educativos y de formación pueden emitir certificados verificables que las personas pueden guardar en sus billeteras digitales. Estas credenciales son a prueba de manipulaciones y fácilmente verificables, útiles para que los solicitantes de empleo demuestren sus cualificaciones a posibles empleadores. Además, estos registros pueden incluir un historial profesional detallado, lo que ayuda a las

personas a crear un currículum verificable al que se puede acceder y compartir de forma segura.

- **Verificación de credenciales de voluntarios/empleados:** Las ONG dependen en gran medida de voluntarios y empleados temporales, y las billeteras digitales pueden agilizar el proceso de verificación de sus credenciales. Al mantener registros digitales de la formación y los antecedentes, las ONG pueden verificar rápidamente la idoneidad de las personas para tareas específicas, mejorando tanto la seguridad como la eficiencia. Este sistema también permite a los trabajadores de las ONG llevar consigo sus credenciales cuando cambian de organización y de función, lo que simplifica el proceso de incorporación.
- **Programas de compromiso y fidelización:** Para fomentar el compromiso continuo, las ONG pueden implantar programas de fidelización a través de billeteras digitales. Los participantes pueden ganar puntos por horas trabajadas, donaciones o participación en programas comunitarios, que pueden canjear por diversas recompensas o reconocimientos públicos. Esto no sólo fomenta una mayor implicación de la comunidad, sino que también proporciona un incentivo tangible para seguir apoyando las actividades de las ONG.

A través de estos casos de uso, las billeteras digitales universales pueden aumentar significativamente las capacidades de las ONG, mejorando la eficiencia, la seguridad y la transparencia de sus operaciones, al tiempo que proporcionan beneficios sustanciales a las comunidades a las que sirven.

A.3. Educación

Las billeteras digitales universales pueden transformar significativamente el sector educativo al mejorar la gestión y accesibilidad de las credenciales

educativas, agilizar los procesos administrativos y facilitar las oportunidades de aprendizaje. He aquí algunos casos de uso específicos para la educación:

- **Almacenamiento seguro de credenciales educativas:** Las billeteras digitales pueden almacenar de forma segura credenciales educativas como diplomas, certificados, expedientes académicos e insignias. Estas credenciales se emiten en un formato digital a prueba de manipulaciones y verificable, lo que facilita a los estudiantes mantener un registro permanente y accesible de sus logros. Esta característica es especialmente beneficiosa cuando los estudiantes solicitan oportunidades de educación superior o empleo, ya que simplifica el proceso de verificación para instituciones y empleadores.
- **Facilitar las microcredenciales y el aprendizaje permanente:** A medida que la educación se orienta hacia vías de aprendizaje más personalizadas y continuas, las billeteras digitales pueden apoyar la tendencia de las microcredenciales. Estas billeteras permiten a los estudiantes recopilar y mostrar una variedad de logros más pequeños, basados en habilidades, que van adquiriendo a lo largo de su vida. Las instituciones educativas pueden emitir estas credenciales verificables directamente en la billetera digital del estudiante, lo que permite un registro dinámico del aprendizaje permanente que es fiable y fácil de compartir.
- **Agilizar los pagos de matrículas y las ayudas financieras:** Las billeteras digitales también pueden gestionar transacciones financieras relacionadas con la educación, como pagos de matrículas, becas y otras formas de ayuda financiera. Esta integración hace que los procesos de pago sean más eficientes y transparentes. Además, las billeteras pueden facilitar un apoyo financiero más personalizado, desembolsando becas o ayudas en función de condiciones específicas o logros almacenados en la billetera.
- **Mayor acceso a los recursos educativos:** Las billeteras digitales pueden utilizarse para autenticar y conceder acceso a diversos recursos e instalaciones educativas. Por ejemplo, una billetera puede contener pases digitales que permitan a los estudiantes acceder a bibliotecas, laboratorios, cursos en línea o contenidos educativos exclusivos. Este sistema garantiza que sólo los estudiantes que cumplan los requisitos puedan acceder a estos recursos, al tiempo que facilita a las instituciones la gestión de los permisos.
- **Comprobación automatizada de la elegibilidad para préstamos estudiantiles:** Mediante el uso de billeteras digitales que contienen credenciales verificables, se puede automatizar el proceso de comprobación de la elegibilidad para los préstamos estudiantiles. Los proveedores de préstamos pueden verificar al instante las calificaciones académicas, el estado de la matrícula y la necesidad financiera directamente desde la billetera digital. Esta automatización no sólo acelera el proceso de solicitud de préstamos, sino que también reduce los gastos administrativos tanto para las instituciones educativas como para los proveedores financieros.
- **Seguimiento de la asistencia y la participación:** Las instituciones educativas pueden utilizar billeteras digitales para controlar la asistencia y la participación en cursos, seminarios y talleres. Esto puede ser especialmente útil en entornos de aprendizaje mixtos o totalmente en línea, en los que los registros digitales pueden sustituir a los métodos tradicionales de pasar lista. La información recopilada también puede ayudar a los educadores y a las instituciones a comprender mejor el compromiso de los estudiantes y la eficacia de los distintos métodos de enseñanza.
- **Fomentar la participación de los estudiantes:** Las billeteras digitales pueden incorporar elementos de gamificación y recompensas para fomentar la participación y los logros de los estudiantes. Por ejemplo, los estudiantes podrían ganar fichas digitales o puntos por logros aca-

démicos, asistencia o participación en actividades extracurriculares, que podrían canjear por diversas recompensas como créditos en la cafetería, descuentos en la librería o privilegios especiales.

Estos casos de uso demuestran cómo las billeteras digitales universales pueden revolucionar el panorama educativo al proporcionar una forma más integrada, segura y eficiente de gestionar y utilizar las credenciales y los recursos educativos. Esta tecnología no solo respalda las necesidades administrativas y operativas de las instituciones educativas, sino que también mejora la experiencia educativa de los estudiantes.

A.4. Salud

Las billeteras digitales universales pueden transformar significativamente el sector sanitario al mejorar la gestión y accesibilidad de los historiales médicos, agilizar los procesos administrativos y facilitar una atención centrada en el paciente. Estos son algunos casos concretos de uso de billeteras digitales universales en el sector sanitario:

- **Almacenamiento seguro de historiales médicos:** Las billeteras digitales pueden almacenar y gestionar de forma segura historiales médicos electrónicos (HCE, por su nombre en inglés), como historiales médicos, resultados de laboratorio, listas de medicación y registros de vacunación. Estos registros se emiten como credenciales verificables, lo que garantiza que son a prueba de manipulaciones y de fácil verificación. Los pacientes pueden conceder a los profesionales sanitarios acceso a sus billeteras para consultar la información médica necesaria, lo que mejora la continuidad de la atención y reduce el riesgo de errores médicos asociados a historiales incompletos de los pacientes.
- **Agilización de las solicitudes de reembolso y los pagos:** Las billeteras digitales pueden simplificar el proceso de presentación de reclamaciones

al seguro médico y la gestión de los pagos. Los pacientes pueden almacenar los datos de su seguro como credenciales verificables en sus billeteras, que pueden compartirse directamente con los proveedores de asistencia sanitaria y las aseguradoras para una rápida verificación y tramitación de las reclamaciones. Esto reduce el papeleo, acelera los plazos de reembolso y disminuye la carga administrativa de los sistemas sanitarios.

- **Facilitar la gestión de las recetas:** Los pacientes pueden recibir recetas digitales almacenadas directamente en sus billeteras, que luego pueden presentar a las farmacias para su cumplimentación. Esto garantiza que las recetas se gestionan de forma segura y ayuda a prevenir el fraude. Además, las billeteras digitales pueden realizar un seguimiento de los horarios de medicación y enviar recordatorios a los pacientes, lo que contribuye al cumplimiento de la medicación por parte del paciente. También puede garantizar que los pacientes no abusen de ciertos medicamentos obteniendo más recetas múltiples para el mismo medicamento.
- **Mayor acceso a los servicios de telemedicina:** Las billeteras digitales pueden autenticar y agilizar el acceso a los servicios de telemedicina. Al almacenar de forma segura las identidades y credenciales médicas de los pacientes, las billeteras garantizan que solo los pacientes que reúnen los requisitos puedan acceder a plataformas de telesalud específicas, al tiempo que proporcionan a los profesionales sanitarios la información necesaria sobre el paciente para prestarle atención personalizada a distancia.
- **Información médica de emergencia:** Las billeteras digitales pueden contener información médica de emergencia, como el grupo sanguíneo, alergias y condiciones críticas de salud, en un formato fácilmente accesible. Esta información puede ser crucial en situaciones de emergencia en las que el acceso rápido a los antecedentes médicos de un paciente es vital para un tratamiento oportuno y eficaz.

- **Promoción de programas de salud y bienestar:** Los proveedores de servicios sanitarios y las aseguradoras pueden utilizar las billeteras digitales para promover programas de salud y bienestar ofreciendo fichas digitales o créditos por lograr hitos de salud, como dejar de fumar o alcanzar objetivos de forma física. Estos incentivos pueden almacenarse en las billeteras digitales y canjearse por beneficios como abonos para gimnasios, vales para comida sana o primas de seguro más bajas.
- **Integración en iniciativas de salud pública:** Las billeteras digitales pueden desempeñar un papel clave en las iniciativas de salud pública almacenando y compartiendo de forma segura credenciales del estado de salud, como registros de vacunación o resultados de pruebas. Esto resulta especialmente útil en la gestión de las respuestas de salud pública durante las pandemias, cuando se exige una prueba de vacunación o de recuperación de la enfermedad para viajar o acceder a espacios públicos.

Al aprovechar las billeteras digitales universales para estos casos de uso relacionados con la salud, el sector sanitario puede alcanzar mayores niveles de eficiencia, seguridad y satisfacción de los pacientes. La portabilidad y accesibilidad de los datos sanitarios a través de billeteras digitales permite a los pacientes asumir un papel activo en la gestión de su salud y agilizar las interacciones con los sistemas sanitarios.

A.5. Instituciones financieras

Las billeteras digitales universales están a punto de revolucionar el sector financiero al permitir interacciones más ágiles, seguras y sencillas entre las entidades financieras y sus clientes. A continuación, se exponen varios casos de uso impactantes, especialmente centrados en cómo los DNI electrónicos (DNLe) equipados con firmas electrónicas cualificadas pueden transformar los procesos contractuales:

- **Firma remota de contratos con alta garantía:** Una de las ventajas más significativas del uso de billeteras digitales en las entidades financieras es la posibilidad de firmar contratos a distancia con el máximo nivel de garantía. Los eID almacenados en las billeteras digitales, especialmente los que incluyen firmas electrónicas cualificadas, cumplen las normas de seguridad más estrictas establecidas por la autoridades reguladoras. Estas firmas tienen el mismo peso legal que las firmas manuscritas tradicionales, pero añaden niveles de seguridad y verificabilidad que superan incluso a los procesos KYC (Conozca a su cliente) presenciales. Las instituciones financieras pueden aprovechar estas capacidades para permitir a los clientes firmar de forma segura documentos bancarios, acuerdos de préstamo y otros contratos desde cualquier lugar y en cualquier momento, sin necesidad de acudir personalmente a una sucursal. Esto no sólo aumenta la comodidad del cliente, sino que también acelera los plazos de tramitación y aprobación de los acuerdos financieros.
- **Agilización de los procesos de verificación de la identidad y KYC:** Las billeteras digitales pueden agilizar significativamente el proceso KYC, un requisito crítico en la industria financiera. Al almacenar credenciales de identidad verificadas, como los documentos de identidad electrónicos y otros datos personales pertinentes, las billeteras digitales permiten a los clientes compartir su información verificada de forma segura con las entidades financieras. Este método elimina la necesidad de comprobaciones repetitivas, reduciendo costes administrativos y mejorando la experiencia del cliente. El alto grado de seguridad que ofrecen los documentos de identidad nacional digitales en estas billeteras digitales garantiza el cumplimiento de los requisitos normativos para KYC y minimiza el riesgo de fraude en los mismos.
- **Autenticación de clientes mejorada:** Las entidades financieras pueden utilizar las billeteras digitales para implantar mecanismos de autenticación más robustos para las transacciones y el acceso a las

cuentas. Los eID de las billeteras digitales equipados con características biométricas, como la huella dactilar o el reconocimiento facial, ofrecen un nivel de seguridad superior al de los métodos tradicionales basados en contraseñas. Esta mayor seguridad es crucial para evitar accesos no autorizados y proteger datos financieros sensibles.

- **Facilitar transacciones de pago seguras:** Las billeteras digitales permiten realizar transacciones de pago seguras y eficientes. Los clientes pueden utilizar sus billeteras para almacenar credenciales de pago e iniciar transacciones rápidamente con un mayor nivel de seguridad. Esta configuración es especialmente beneficiosa para la banca en línea y los pagos por móvil, donde la facilidad de uso y la seguridad son primordiales.
- **Servicios financieros personalizados:** Con el acceso a datos precisos y seguros de los clientes que proporcionan las billeteras digitales, las instituciones financieras pueden ofrecer servicios bancarios y financieros más personalizados. Basándose en el perfil completo creado a partir de las credenciales almacenadas y el historial de transacciones del cliente, los bancos pueden adaptar sus ofertas, como préstamos, tipos de interés y asesoramiento en materia de inversión, a las necesidades y los perfiles de riesgo de cada cliente.
- **Cumplimiento de la normativa y presentación de informes:** Las billeteras digitales equipadas con eID simplifican el cumplimiento de los requisitos normativos, incluida la normativa contra el blanqueo de capitales (AML) y la financiación del terrorismo (CTF). Las instituciones financieras podrán solicitar y verificar en tiempo real los registros que los particulares almacenan y presentan desde sus billeteras digitales.
- **Calificación crediticia y análisis de riesgos:** Las billeteras digitales universales equipadas con credenciales verificables de educación, salud, seguros y otros sectores ofrecen una herramienta sólida para que

las instituciones financieras perfeccionen sus procesos de puntuación crediticia y análisis de riesgos. Las personas pueden proporcionar de forma segura estas credenciales verificadas a los prestamistas, lo que permite una evaluación más completa de su fiabilidad financiera y perfil de riesgo. Esta integración no sólo enriquece la precisión de las evaluaciones crediticias, sino que también permite tomar decisiones de préstamo más personalizadas, aumentando potencialmente el acceso al crédito.

- **Facilitar los mercados secundarios de activos tokenizados:** Las billeteras digitales no solo gestionan activos tokenizados, sino que también facilitan su intercambio en mercados secundarios. Los mercados podrán integrarse directamente con las billeteras digitales, verificando las identidades de los usuarios para llevar a cabo el KYC y AML con conformidad. Los usuarios podrán comprar y vender fácilmente activos al instante que representen diferentes tipos de valor a través de estos mercados.

Al integrar las billeteras digitales universales con los DNI electrónicos y las firmas electrónicas cualificadas, las entidades financieras pueden reducir costes y prevenir el fraude mejorando los procesos de verificación de la identidad, además de garantizar altos niveles de seguridad y el cumplimiento de las normativas vigentes. Asimismo, al aprovechar las capacidades de las billeteras digitales en el manejo de activos tokenizados, las instituciones financieras pueden ofrecer servicios más flexibles, accesibles y eficientes a sus clientes.

A.6 Marketing y publicidad

Las billeteras digitales universales están a punto de transformar los sectores del marketing y la publicidad al servir de plataformas dinámicas para promocionar servicios y productos. Esta transformación es especialmente potente cuando se combina con el consentimiento del usuario, lo que garantiza que las promociones sean específicas y pertinentes. He aquí

cómo las billeteras digitales pueden mejorar las estrategias de marketing y publicidad:

- **Publicidad dirigida y basada en el consentimiento:** Las billeteras digitales equipados con mecanismos de consentimiento del usuario brindan a las empresas una oportunidad única de relacionarse directamente con los consumidores de forma personalizada. Al obtener el consentimiento explícito, las empresas pueden asegurarse de que sus esfuerzos publicitarios no sólo cumplen la normativa sobre privacidad, sino que también tienen más probabilidades de ser bien recibidos por la audiencia. Este enfoque basado en el consentimiento permite a las empresas adaptar sus mensajes de marketing en función de las preferencias y comportamientos específicos de los usuarios de la billetera, lo que conduce a mayores tasas de compromiso y conversión.
- **Integración perfecta de programas de fidelización y premios:** Las billeteras digitales pueden integrar perfectamente varios programas de recompensas y fidelización, ofreciendo a los usuarios acceso instantáneo a recompensas, descuentos u ofertas especiales directamente desde la interfaz de la billetera. Esta integración fomenta el compromiso continuo entre empresas y clientes, reforzando la fidelidad a la marca. Por ejemplo, después de hacer una compra, un cliente puede recibir fichas digitales o puntos en su billetera, que pueden canjearse por descuentos en futuras compras o acceso exclusivo a nuevos productos.
- **Mayor conocimiento del cliente:** La gran cantidad de datos disponibles a través de las billeteras digitales puede proporcionar a las empresas una visión más profunda de los comportamientos y preferencias de los consumidores. Con el consentimiento del usuario, las empresas pueden analizar los historiales de compra y las interacciones con la billetera para perfeccionar sus estrategias de marketing y desarrollar campañas más específicas. Este enfoque basado en los datos permite a las empresas ofrecer experiencias altamente personalizadas, mejorando la satisfacción del cliente y la fidelidad a la marca.
- **Canales de comunicación directa:** Las billeteras digitales permiten a las empresas establecer canales de comunicación directa con los usuarios, facilitando notificaciones oportunas y relevantes sobre nuevos productos, servicios o promociones. Esta interacción directa garantiza que los mensajes de marketing lleguen directamente al dispositivo móvil del consumidor, lo que aumenta la visibilidad y el impacto de los esfuerzos publicitarios.
- **Promociones geolocalizadas:** Utilizando los servicios de localización de las billeteras digitales, las empresas pueden activar promociones geolocalizadas cuando un usuario de billetera se encuentra cerca de una tienda o ubicación concreta. Esta capacidad permite un marketing altamente contextual y oportuno que puede mejorar significativamente la eficacia de las campañas promocionales.
- **Monetización de la participación y los datos de los usuarios:** Las billeteras digitales podrían permitir a los usuarios monetizar su exposición a los anuncios y su participación en actividades de marketing, de forma similar a como los creadores de contenidos ganan con las visitas y la participación en las redes sociales. Los usuarios podrían participar en programas de marketing en los que recibirían una compensación por ver anuncios, compartir datos o participar en estudios de mercado directamente a través de sus billeteras. Esta configuración convierte la atención y los datos en activos tangibles que los usuarios pueden controlar y de los que pueden beneficiarse, creando potencialmente una nueva fuente de ingresos para los consumidores de a pie.
- **Facilitar las transacciones con pagos integrados:** La integración de las funcionalidades de identidad y pago en las billeteras digitales

simplifica considerablemente las transacciones. Cuando un usuario decide comprar un producto o servicio anunciado a través de la billetera, la presencia de métodos de pago almacenados y credenciales de identidad permite realizar transacciones seguras y sin problemas. Esta integración elimina la necesidad de introducir la información de pago varias veces, lo que reduce la fricción y mejora la experiencia del usuario. Para los anunciantes, esto significa mayores tasas de conversión, ya que se minimizan las barreras a la compra.

Las billeteras digitales universales, por tanto, representan una herramienta versátil para el marketing y la publicidad, permitiendo a las empresas relacionarse con los consumidores de una manera más personalizada, eficiente y respetuosa con el medio ambiente. Con la dimensión añadida del consentimiento del usuario, estas interacciones no sólo son más específicas, sino también más respetuosas con la privacidad del usuario, en consonancia con las expectativas de los consumidores contemporáneos y las normas reguladoras. Aprovechando los sistemas integrados de identidad y pago, las billeteras digitales universales podrían revolucionar la forma en que los usuarios interactúan con los anunciantes, creando un ecosistema más dinámico, personalizado y rentable. Este enfoque no sólo beneficia a los usuarios al proporcionarles control e ingresos potenciales, sino que también ofrece a los anunciantes formas más eficaces de llegar y captar a su público objetivo.

A.7. Criptomonedas, *Stablecoins* y CBDC

Las billeteras digitales universales están revolucionando las transacciones financieras al aprovechar las capacidades de las criptomonedas, las *stablecoins* (o monedas estables) y las monedas digitales de bancos centrales (CBDC). Estos activos digitales, cuando se integran en las billeteras universales, ofrecen una serie de ventajas que agilizan las transacciones, mejoran la accesibilidad y garantizan el cumplimiento de la normativa

internacional. A continuación, algunos ejemplos de cómo se manifiestan estas ventajas en diversas aplicaciones:

- **Comodidad para las transacciones entre pares:** Las billeteras digitales universales simplifican las transacciones peer-to-peer (P2P) al permitir a los usuarios transferir directamente monedas digitales como criptomonedas, *stablecoins* y CBDC entre sí sin necesidad de intermediarios para liquidar esas transacciones -aunque los intermediarios son necesarios para habilitar interfaces como intercambios, billeteras o creación de activos digitales-. Esta capacidad de transferencia directa reduce los tiempos y costes de las transacciones, lo que hace excepcionalmente cómodo para los usuarios enviar y recibir pagos de forma instantánea y segura.
- **Pagos sin fisuras en comercios:** Al admitir transacciones de criptomonedas, *stablecoins* y CBDC, las billeteras digitales universales permiten a los consumidores utilizar estos activos digitales para las compras cotidianas. Esta integración permite procesos de pago sin fisuras en las tiendas de los comerciantes, tanto en línea como fuera de línea, proporcionando una experiencia de pago rápida y fácil. Los comercios se benefician de comisiones de transacción más bajas en comparación con los pagos tradicionales con tarjeta de crédito y obtienen acceso a una base más amplia de particulares.
- **Pagos transfronterizos y remesas eficientes:** Las billeteras digitales universales facilitan pagos transfronterizos más baratos y rápidos aprovechando las eficiencias inherentes de las criptomonedas y las *stablecoins*. Estos activos digitales eluden los complejos y cargados de comisiones sistemas bancarios tradicionales, permitiendo a los usuarios realizar transacciones internacionales que no sólo son rentables, sino también más rápidas. Para las remesas, esto significa que los trabajadores en el extranjero pueden enviar dinero a casa de manera más eficiente, maximizando los fondos que llegan a sus familias.

- **Cumplimiento de la normativa:** El cumplimiento de normativas como la Crypto Travel Rule se agiliza en las billeteras digitales universales. Estas billeteras están diseñadas para gestionar y proteger la información de identidad del usuario junto con sus transacciones financieras, garantizando que todos los datos necesarios acompañan a las transferencias para cumplir las normas mundiales contra el blanqueo de capitales y la financiación del terrorismo. Este enfoque integrado ayuda a mantener el equilibrio necesario entre la privacidad del usuario y el cumplimiento de la normativa.
- **Mayor inclusión financiera:** Las billeteras digitales universales, especialmente los que apoyan los CBDC, desempeñan un papel fundamental en la mejora de la inclusión financiera. Proporcionan a las poblaciones no bancarizadas y sub-bancarizadas acceso a los servicios financieros digitales y a las monedas digitales respaldadas por el gobierno. Esta accesibilidad ayuda a integrar a un mayor segmento de la población en el sistema financiero formal, proporcionándoles las herramientas necesarias para una participación económica mejorada.

Al integrar criptomonedas, *stablecoins* y CBDC, las billeteras digitales universales no solo mejoran la funcionalidad y el alcance de los servicios financieros tradicionales, sino que también introducen un nuevo paradigma en las transacciones financieras que es seguro, inclusivo y alineado con la era digital. Este enfoque integral de la gestión de activos digitales pone de manifiesto el potencial de las billeteras digitales universales para transformar el panorama financiero mundial.

A.8. Comunidades y ecosistemas

Las billeteras digitales universales están llamados a redefinir las interacciones entre comunidades y ecosistemas facilitando la identificación segura, el acceso sin fisuras y la gobernanza participativa. A continuación, algunos

ejemplos de como estas billeteras pueden aportar beneficios tangibles a diversas actividades impulsadas por la comunidad:

- **Identificación digital de los miembros:** Las billeteras digitales universales pueden almacenar identificaciones digitales de los miembros que sirven como prueba de identidad dentro de una comunidad o ecosistema. Estas identificaciones pueden utilizarse para la autenticación física y digital, garantizando que solo los miembros autorizados accedan a determinados servicios o lugares.
- **Acceso basado en códigos QR:** Las billeteras pueden facilitar la entrada a eventos o el acceso a servicios mediante el escaneo de códigos QR. Este método rápido y seguro permite a los miembros autenticar su identidad simplemente escaneando un código QR con su dispositivo móvil, agilizando el proceso de entrada y mejorando la comodidad del usuario.
- **Adquisición y canje de beneficios:** Las billeteras digitales permiten a las comunidades distribuir beneficios o recompensas directamente a las billeteras de sus miembros. Pueden incluir descuentos, créditos o acceso a servicios exclusivos. Los miembros pueden canjear estos beneficios sin esfuerzo, ya sea en línea o en lugares físicos, fomentando el compromiso y la lealtad dentro de la comunidad.
- **Ofertas e incentivos personalizados:** Basándose en el historial de transacciones y las preferencias almacenadas en sus billeteras digitales, los miembros pueden recibir ofertas e incentivos personalizados. Esto no solo mejora la experiencia de los socios, sino que también permite a las comunidades apoyar mejor a las empresas locales dirigiendo el tráfico de consumidores hacia ellas mediante promociones específicas.
- **Votación digital para decisiones comunitarias:** Las billeteras digitales pueden revolucionar la gobernanza dentro de las comunidades al facilitar

mecanismos de votación digital seguros y transparentes. Los miembros pueden votar sobre asuntos comunitarios desde sus dispositivos, garantizando una amplia participación y compromiso en los procesos de toma de decisiones. La inmutabilidad de la tecnología blockchain, a menudo integrada en estas billeteras, garantiza que cada voto se cuente y sea inviolable.

- **Gobernanza participativa:** Al permitir el voto digital, las billeteras digitales universales capacitan a los miembros de la comunidad para asumir un papel activo en la gobernanza. Este enfoque participativo puede extenderse a diversos aspectos de la gestión comunitaria, desde la elección de representantes hasta la toma de decisiones sobre proyectos comunitarios y asignaciones presupuestarias.
- **Aprovechamiento de las redes de afiliados:** Las billeteras digitales universales agilizan la gestión de las afiliaciones y el acceso a las ventajas dentro de las comunidades y las redes de afiliados. Al centralizar los procesos de inscripción y autenticación, estas billeteras simplifican la forma en que los miembros reciben y canjean las ventajas, se inscriben en los servicios y acceden a los descuentos. Además, permiten una verificación segura y sin fisuras de los descuentos y ofertas exclusivas de las redes afiliadas, lo que aumenta la comodidad y el valor de la participación en la comunidad. Esta integración no sólo fomenta la fidelidad, sino que también garantiza el fácil acceso a las ventajas, promoviendo ecosistemas más comprometidos y conectados.

A.9. Servicios para Corporativos

Las billeteras digitales universales tienen el potencial de agilizar las transacciones financieras, mejorar la gestión de los beneficios de los empleados y facilitar el acceso seguro a los recursos corporativos. A continuación, varias aplicaciones clave de las billeteras digitales en un entorno corporativo:

- **Mejores beneficios y recompensas para los empleados:** Las empresas pueden utilizar las billeteras digitales para gestionar y distribuir los beneficios de los empleados de forma más eficiente. Esto podría incluir prestaciones sanitarias, seguros, cuentas de jubilación o incluso cuentas de gastos flexibles. Las billeteras digitales también pueden utilizarse para distribuir recompensas basadas en el rendimiento, directamente a la billetera del empleado, mejorando la transparencia y la inmediatez.
- **Acceso seguro a sistemas corporativos:** Las billeteras digitales pueden servir como herramientas de autenticación segura para acceder a los sistemas e instalaciones corporativos. Al integrar datos biométricos como huellas dactilares o reconocimiento facial, las billeteras digitales pueden garantizar que sólo el personal autorizado acceda a información sensible o a ubicaciones físicas. Esto no sólo aumenta la seguridad, sino que también proporciona a los empleados una forma cómoda de acceder a los recursos que necesitan sin tener que gestionar múltiples contraseñas o contraseñas físicas.
- **Programas corporativos personalizados:** Las empresas pueden aprovechar las billeteras digitales para crear programas personalizados de fidelización o incentivos que fomenten los comportamientos deseados entre los empleados. Por ejemplo, pueden ofrecerse recompensas por completar módulos de formación, alcanzar objetivos de ventas o participar en iniciativas de bienestar corporativo.

Al integrar las billeteras digitales universales, las empresas pueden lograr una mayor eficiencia operativa, mejorar la satisfacción de los empleados y aumentar la seguridad en todos sus procesos de gestión financiera y de recursos humanos. Esta tecnología no solo agiliza las funciones corporativas tradicionales, sino que también abre nuevas vías para la innovación en el compromiso de los empleados.

A.10. Eventos

Las billeteras digitales universales pueden mejorar significativamente la experiencia de organizar y asistir a eventos agilizando las transacciones, gestionando el acceso y facilitando las interacciones entre los participantes. A continuación, algunos ejemplos de cómo pueden utilizarse eficazmente las billeteras digitales en el contexto de los eventos:

- **Venta de entradas y control de acceso:** Las billeteras digitales pueden transformar el proceso de venta de entradas para eventos almacenando las entradas digitales de forma segura. Estas entradas pueden comprarse directamente a través de la billetera y almacenarse junto con otras credenciales digitales, garantizando un acceso y una verificación sencillos a la entrada del evento. Este sistema elimina la necesidad de entradas físicas, reduciendo el desperdicio y la posibilidad de pérdida o robo. Además, gracias a la verificación de identidad integrada, los organizadores de eventos pueden garantizar que sólo acceden los titulares de las entradas, lo que mejora la seguridad y agiliza el proceso de registro.
- **Pagos sin efectivo en eventos:** En muchos eventos, desde conciertos a conferencias, los participantes pueden beneficiarse de las opciones de pago sin efectivo. Las billeteras digitales permiten a los asistentes realizar compras in situ sin necesidad de efectivo ni tarjetas de crédito físicas. Tanto si compran productos, comida o participan en actividades de pago, las transacciones pueden realizarse de forma rápida y segura a través de sus billeteras digitales. Esto no sólo aumenta la comodidad para los asistentes, sino que también simplifica la gestión de las transacciones para los proveedores, reduciendo las colas y mejorando la eficiencia general del evento.
- **Redes e intercambio de información:** En los eventos profesionales y de networking, las billeteras digitales pueden facilitar el intercambio

de información de contacto y tarjetas de visita digitales. Los asistentes pueden compartir sus perfiles profesionales y datos de contacto a través de sus billeteras, lo que hace que el networking sea más eficiente y ecológico al eliminar las tarjetas de visita de papel. Además, los organizadores pueden utilizar las billeteras digitales para distribuir programas de eventos, actualizaciones y materiales directamente a los dispositivos de los asistentes.

- **Ofertas y promociones personalizadas:** Los organizadores de eventos pueden utilizar las billeteras digitales para enviar ofertas, actualizaciones y promociones personalizadas directamente a los asistentes en función de sus preferencias y comportamientos anteriores. Por ejemplo, si un asistente ha expresado interés por un ponente o un producto en particular, podría recibir notificaciones sobre sesiones o productos relacionados. Esta comunicación personalizada puede mejorar la experiencia de los asistentes y aumentar su participación.
- **Programas de fidelización para asistentes frecuentes:** Para eventos recurrentes o series de eventos, las billeteras digitales pueden gestionar programas de fidelización que recompensen a los asistentes frecuentes. Los beneficios pueden incluir descuentos en futuras entradas, acceso exclusivo a determinadas zonas o sesiones, o productos especiales. Las recompensas por fidelidad pueden gestionarse directamente desde la billetera, lo que fomenta el compromiso continuo y mejora la fidelidad a la marca entre los asistentes.

En resumen, las billeteras digitales universales ofrecen multitud de ventajas para la gestión de eventos y la asistencia a los mismos, desde la entrada y las transacciones seguras hasta la mejora de los contactos y las experiencias personalizadas de los usuarios y empleados del evento.

A.11. Gaming

Las billeteras digitales universales tienen el potencial de transformar significativamente la industria del juego al mejorar la forma en que los jugadores compran, intercambian y gestionan los activos digitales, además de agilizar los pagos y las recompensas dentro de los ecosistemas de juego. A continuación, se explica cómo pueden utilizarse eficazmente las billeteras digitales en este contexto:

- **Compras dentro del juego y gestión de divisas:** Las billeteras digitales permiten a los jugadores gestionar las monedas del juego y realizar compras sin problemas. Ya se trate de comprar bienes virtuales, mejorar funciones o desbloquear nuevos niveles, las transacciones pueden realizarse de forma rápida y segura dentro de la interfaz del juego. Esta integración no sólo mejora la experiencia del usuario al simplificar el proceso de compra, sino que también ayuda a los desarrolladores de juegos a gestionar las transacciones de forma más eficaz y segura.
- **Intercambio y venta de bienes virtuales:** Los jugadores pueden utilizar billeteras digitales para almacenar bienes virtuales como skins, armas, personajes o cualquier otro activo intercambiable dentro del juego. Estas billeteras facilitan el comercio o la venta segura y eficiente de estos artículos entre jugadores, potencialmente en una plataforma de mercado integrada proporcionada por los desarrolladores del juego. Esta capacidad añade una capa de actividad económica, enriqueciendo la experiencia de usuario y ofreciendo a los jugadores un valor tangible por sus logros en el juego.
- **Compatibilidad entre juegos y portabilidad:** Las billeteras digitales admiten la compatibilidad entre juegos, lo que permite a los jugadores transferir determinados activos de un juego a otro dentro del mismo ecosistema de juego. Esta característica es especialmente atractiva, ya que añade valor a las compras y actividades de los jugadores,

mejorando la lealtad y el compromiso a través de diferentes juegos desarrollados por la misma empresa o desarrolladores afiliados.

- **Recompensas y programas de fidelización:** Las plataformas de juego pueden integrar programas de fidelización directamente en las billeteras digitales, con los que los jugadores obtienen recompensas en función de su actividad o sus logros en el juego. Estas recompensas pueden consistir en contenidos exclusivos, moneda del juego o descuentos especiales en futuras compras. La gestión de estas recompensas a través de una billetera digital facilita a los jugadores ver y canjear sus recompensas, fomentando el compromiso continuado.
- **Mayor seguridad en las transacciones:** Con las transacciones financieras significativas ahora comunes en el juego, las billeteras digitales proporcionan características de seguridad mejoradas como el cifrado y métodos de autenticación seguros para proteger los fondos de los jugadores y los activos virtuales. Esta seguridad es crucial, no solo para mantener la confianza de los jugadores, sino también para cumplir las normas reguladoras relacionadas con las monedas virtuales y las transacciones en línea.

La incorporación de billeteras digitales universales al sector del juego ofrece grandes ventajas tanto a los jugadores como a los desarrolladores. No solo simplifica las interacciones financieras dentro del ecosistema del juego, sino que también mejora la experiencia de juego en general al proporcionar formas seguras, eficientes e innovadoras de gestionar y valorar los activos digitales y las divisas.

A.12. Comercio electrónico

Las billeteras digitales universales están remodelando el panorama del comercio electrónico al agilizar los procesos de transacción, mejorar la seguridad y ofrecer una experiencia de compra más personalizada. A

continuación, algunos ejemplos de cómo se están utilizando eficazmente las billeteras digitales en el contexto del comercio electrónico:

- **Procesos de pago simplificados:** Las billeteras digitales simplifican enormemente el proceso de pago al almacenar la información de pago de forma segura, lo que permite transacciones más rápidas con menos pasos. Los consumidores pueden completar sus compras con un solo clic, sin necesidad de introducir cada vez los datos de la tarjeta de crédito o la información de envío. Esta comodidad no sólo mejora la experiencia del cliente, sino que también reduce las tasas de abandono de carritos, lo que aumenta las ventas.
- **Integración de programas de fidelización y descuentos:** Las empresas pueden integrar sus programas de fidelización y descuentos directamente en las billeteras digitales. Los consumidores pueden aplicar automáticamente los cupones correspondientes, canjear puntos o beneficiarse de ofertas especiales en el momento de pagar, todo ello dentro de la aplicación de su billetera. Esta integración perfecta fomenta el uso repetido de la billetera digital y favorece la fidelidad del cliente al facilitar el acceso a los ahorros.
- **Compatibilidad con múltiples métodos de pago y divisas:** Las billeteras digitales universales pueden aceptar una variedad de métodos de pago, incluidas tarjetas de crédito, transferencias bancarias e incluso criptomonedas. También facilitan las transacciones en varias divisas, lo que resulta especialmente beneficioso para las plataformas internacionales de comercio electrónico. Esta versatilidad hace que las billeteras digitales sean una opción atractiva para los consumidores que buscan flexibilidad y comodidad en sus opciones de pago.
- **Facilitar devoluciones y reembolsos:** Las billeteras digitales pueden agilizar el proceso de devoluciones y reembolsos manteniendo un re-

gistro de las transacciones y facilitando la anulación de los cargos. Esto simplifica la logística de gestión de devoluciones para las empresas y mejora la satisfacción del cliente al hacer que los reembolsos sean rápidos y sencillos.

- **Marketing selectivo y personalización:** Analizando los datos de las transacciones almacenados en las billeteras digitales, los comercios pueden ofrecer experiencias de compra personalizadas y promociones específicas. Por ejemplo, si una billetera indica compras frecuentes de un determinado tipo de producto, la plataforma de comercio electrónico puede ofrecer recomendaciones a medida y descuentos personalizados, mejorando la experiencia de compra y aumentando la probabilidad de nuevas compras.

La adopción de billeteras digitales universales dará lugar a una autenticación digital fiable, una mayor eficiencia, una mejora de la satisfacción del cliente y nuevas formas de gestionar los pagos y las promociones. Esta tecnología no solo agiliza las transacciones financieras, sino que también sirve como herramienta para una mayor implicación de los clientes y el crecimiento empresarial en el espacio del comercio digital.



Referencias

- [1] <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/infographic-what-is-good-digital-id>
- [2] <https://www.javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis#:~:text=Traditional%20identity%20fraud%20losses%20amounted,imperceptible%20drop%20in%20financial%20loss.>
- [3] <https://www.javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis#:~:text=Traditional%20identity%20fraud%20losses%20amounted,imperceptible%20drop%20in%20financial%20loss.>
- [4] <https://b2b.mastercard.com/news-and-insights/blog/ecommerce-fraud-trends-and-statistics-merchants-need-to-know-in-2024/#:~:text=Global%20ecommerce%20fraud%20is%20increasing,exceed%20%2448%20billion%20in%202023.>
- [5] <https://www.coindesk.com/business/2023/10/26/jpmorgan-handles-1b-transactions-daily-in-digital-token-jpm-coin-bloomberg/>
- [6] <https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/the-tides-of-tokenization>
- [7] <https://cointelegraph.com/news/killer-use-case-citi-says-trillions-in-assets-could-be-tokenized-by-2030>
- [8] <https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad-2cb3113a291222/on-chain-asset-tokenization.pdf>
- [9] <https://cbdctracker.org>
- [10] <https://e-estonia.com/solutions/e-governance/e-services-registries/>
- [11] https://www.business-standard.com/india-news/aadhaar-data-of-millions-of-indians-put-on-sale-on-the-dark-web-reports-123103000993_1.html
- [12] https://diacc.ca/wp-content/uploads/2019/02/Pan-Canadian-Trust-Framework-Model-Overview_Discussion-Draft_V0.02.pdf
- [13] https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF
- [14] <https://www.iso.org/home.html>
- [15] <https://www.w3.org>
- [16] <https://openid.net>
- [17] <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>
- [18] <https://www.nfcw.com/2023/06/16/384349/department-of-homeland-security-issues-call-for-digital-wallet-proposals/>
- [19] <https://blog.spruceid.com/spruceid-partners-with-ca-dmv-on-mdl/>
- [20] <https://arxiv.org/html/2408.07892v1>
- [21] <https://www.nature.com/articles/s41598-023-32701-6>
- [22] <https://www.weforum.org/publications/quantum-computing-governance-principles/>
- [23] <https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers>
- [24] <https://csrc.nist.gov/projects/post-quantum-cryptography>



2024