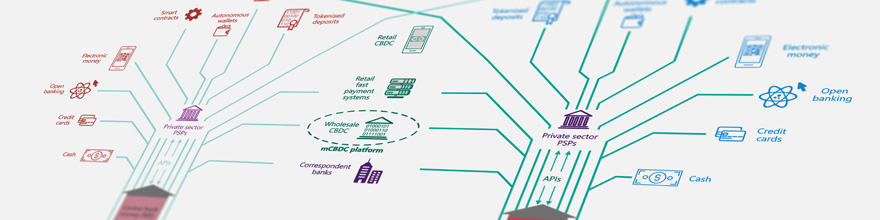
El futuro sistema monetario



**Informe Económico Anual del BIS** | **21 junio 2022**

[**Versión PDF** (1,314kb)](https://www.bis.org/publ/arpdf/ar2022e3.pdf)  |  41 páginas

**Conclusiones clave**

* Se está produciendo una explosión de innovación creativa en dinero y pagos, abriendo perspectivas de un futuro sistema monetario digital que se adapta continuamente para servir al interés público.
* Los defectos estructurales hacen que el universo criptográfico no sea adecuado como base para un sistema monetario: carece de un ancla nominal estable, mientras que los límites a su escalabilidad resultan en fragmentación. Contrariamente a la narrativa de la descentralización, la criptografía a menudo se basa en intermediarios no regulados que plantean riesgos financieros.
* Un sistema basado en el dinero del banco central ofrece una base más sólida para la innovación, asegurando que los servicios sean estables e interoperables, a nivel nacional y transfronterizo. Tal sistema puede mantener un círculo virtuoso de confianza y adaptabilidad a través de efectos de red.
* Las nuevas capacidades, como la programabilidad, la componibilidad y la tokenización, no son patrimonio de la criptografía, sino que se pueden construir sobre las monedas digitales del banco central (CBDC), los sistemas de pago rápido y las arquitecturas de datos asociadas.

**Introducción**

Cada día, personas de todo el mundo realizan más de 2 mil millones de pagos digitales.1 Pagan por bienes y servicios, piden prestado y ahorran y participan en una multitud de transacciones financieras. Cada vez que lo hacen, confían en el sistema monetario, el conjunto de instituciones y arreglos que rodean y apoyan el intercambio monetario.

En el corazón del sistema monetario se encuentra el banco central. A medida que el banco central emite dinero y mantiene sus funciones principales, la confianza en el sistema monetario se basa en última instancia en la confianza en el banco central. Sin embargo, el banco central no opera de forma aislada. Los bancos comerciales y otros proveedores privados de servicios de pago (PSP) ejecutan la gran mayoría de los pagos y ofrecen servicios orientados al cliente. Esta división de roles promueve la competencia y da pleno juego al ingenio y la creatividad del sector privado en el servicio a los clientes. De hecho, la innovación del sector privado beneficia a la sociedad precisamente porque se basa en los sólidos cimientos del banco central.

El sistema monetario con el banco central en su centro ha servido bien a la sociedad. Sin embargo, la innovación digital está ampliando la frontera de las posibilidades tecnológicas, imponiendo nuevas demandas al sistema.

Las innovaciones de gran alcance, como las del universo criptográfico, implican una desviación radical. El universo criptográfico se basa en la premisa de la descentralización. En lugar de depender del dinero del banco central y de intermediarios de confianza, la criptografía prevé controles y equilibrios proporcionados por una multitud de validadores anónimos para mantener el sistema autosuficiente y libre de la influencia de entidades o grupos poderosos. Las finanzas descentralizadas, o "DeFi", buscan replicar los servicios financieros convencionales dentro del universo criptográfico. Estos servicios están habilitados por innovaciones como la programabilidad y la compatibilidad (ver glosario) en blockchains sin permiso. Tales sistemas están "siempre encendidos", lo que permite transacciones globales las 24 horas del día, los 7 días de la semana, basadas en código abierto y sin conocer fronteras.

Sin embargo, los eventos recientes han revelado un gran abismo entre la visión criptográfica y su realidad. La implosión de la moneda estable TerraUSD y el colapso de su moneda gemela Luna han subrayado la debilidad de un sistema que se sostiene mediante la venta de monedas para la especulación. Además, ahora está quedando claro que las criptomonedas y Los DeFi tienen limitaciones estructurales más profundas que les impiden alcanzar los niveles de eficiencia, estabilidad o integridad requeridos para un sistema monetario adecuado. En particular, el universo criptográfico carece de un ancla nominal, que intenta importar, imperfectamente, a través de stablecoins. También es propenso a la fragmentación, y sus aplicaciones no pueden escalar sin comprometer la seguridad, como lo demuestran su congestión y tarifas exorbitantes. La actividad en este sistema paralelo es, en cambio, sostenida por la afluencia de titulares de monedas especulativas. Por último, existen serias preocupaciones sobre el papel de los intermediarios no regulados en el sistema. Como están profundamente arraigadas, es poco probable que estas deficiencias estructurales sean susceptibles de correcciones técnicas por sí solas. Esto se debe a que reflejan las limitaciones inherentes de un sistema descentralizado construido sobre cadenas de bloques sin permiso.

Este capítulo establece una visión alternativa para el futuro, una que se basa en los bienes públicos del banco central. Esto garantizará que los servicios innovadores del sector privado estén firmemente arraigados en la confianza proporcionada por el dinero del banco central.

Escalando sobre la base de los efectos de red, las monedas digitales del banco central (CBDC) y los sistemas de pago rápido minorista (FPS) están bien posicionados para servir al interés público a través de una mayor conveniencia y menores costos, al tiempo que mantienen la integridad del sistema. La descentralización y la tecnología de contabilidad distribuida autorizada (DLT) también pueden desempeñar un papel constructivo, por ejemplo, cuando los bancos centrales trabajan juntos en acuerdos de múltiples CBDC. Estos innovadores carriles de pago son totalmente compatibles con la programabilidad, la compatibilidad y la tokenización para respaldar pagos y liquidaciones más rápidos, seguros y baratos, tanto dentro como fuera de las fronteras. De esta manera, el futuro sistema monetario será adaptable, permitiendo que la innovación del sector privado florezca al tiempo que evita los inconvenientes de la criptografía. Tales iniciativas podrían abrir un nuevo capítulo en el sistema monetario mundial.

Este capítulo está organizado de la siguiente manera. Para sentar las bases, en primer lugar, describe el sistema monetario actual y los objetivos de alto nivel que debe alcanzar, y hasta qué punto los cambios en la tecnología y el entorno económico han abierto un margen de mejora. La siguiente sección discute la promesa y las trampas de las innovaciones criptográficas y DeFi. El capítulo luego discute una visión para el futuro sistema monetario, construido sobre los bienes públicos del banco central. La sección final concluye.

**¿Qué queremos de un sistema monetario?**

El sistema monetario es el conjunto de instituciones y arreglos que apoyan el intercambio monetario. Consiste en dinero y sistemas de pago.2 ¿Qué se requiere de tal sistema para servir a la sociedad? Si bien no existe una lista canónica de características necesarias, se destacan una serie de objetivos de alto nivel ([Tabla 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-tab1), primera columna).

Para garantizar la **seguridad y estabilidad** del sistema, el dinero debe cumplir tres funciones: como reserva de valor, unidad de cuenta y medio de intercambio. Cuando el sistema monetario se basa en nodos o entidades clave (ya sean públicas o privadas), deben **rendir cuentas**, a través de mandatos específicos para las autoridades públicas y a través de una regulación y supervisión adecuadas para las entidades privadas. El sistema monetario debe ser **eficiente**, permitiendo pagos fiables y rápidos para apoyar las transacciones económicas tanto a escala como a bajo coste. El acceso a los servicios básicos de pago a precios asequibles, en particular las cuentas de transacción, debe ser universal para difundir los beneficios de la actividad económica, promoviendo la **inclusión financiera**. No menos importante, el sistema debe proteger la privacidad como un derecho fundamental y proporcionar **control al usuario sobre los** datos financieros. La **integridad** del sistema debe protegerse, protegiéndose contra actividades ilícitas como el lavado de dinero, el financiamiento del terrorismo y el fraude.

**Cuadro 1**



El sistema monetario no es sólo una instantánea de la economía tal como existe hoy en día; necesita evolucionar con cambios estructurales en la economía y la sociedad. Por esta razón, los medios para alcanzar los objetivos de alto nivel establecidos en el [cuadro 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-tab1) deben evolucionar con el propio sistema monetario y la tecnología que lo sustenta. En resumen, el sistema monetario debe ser **adaptable**: debe *anticiparse a* los desarrollos futuros y a las necesidades de los usuarios. Debe estar en sintonía con los avances tecnológicos y responder a las demandas cambiantes de los hogares y las empresas, y debe fomentar la competencia y la innovación. Para servir mejor a un mundo cada vez más interconectado, el sistema monetario también debe ser **abierto**, interoperable y flexible, tanto a nivel nacional como transfronterizo. Así como las transacciones económicas trascienden las fronteras, el sistema monetario tendrá que servir a una red sin fisuras de entidades interconectadas, en lugar de islas de actividad escasamente conectadas.

El sistema monetario actual ha recorrido algún camino hacia estos objetivos de alto nivel, pero todavía queda camino por recorrer. Los cambios en las necesidades de los usuarios y los cambios concomitantes en la tecnología han apuntado a áreas de mejora ([Tabla 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-tab1), segunda columna). Los servicios de pago actuales a veces pueden ser engorrosos y costosos de usar, en parte reflejando la falta de competencia. Los pagos transfronterizos son particularmente caros, opacos y lentos: generalmente involucran a uno o más bancos corresponsales para liquidar una transacción, utilizando libros de contabilidad basados en diferentes tecnologías.3 Además, una gran parte de los adultos, especialmente en las economías de mercados emergentes y en desarrollo, todavía no tienen acceso a las opciones de pago digital. Pero un mundo globalizado que presenta una economía digital en constante crecimiento requiere un sistema monetario que permita a todos realizar transacciones financieras a nivel nacional y mundial de una manera segura, sólida y eficiente. Atender a estos cambios en las demandas que la sociedad pone en el sistema monetario requiere avances en la tecnología y los arreglos institucionales.

**La promesa y las trampas de la criptografía**

El universo criptográfico está en crisis. La implosión de la stablecoin TerraUSD y su moneda gemela Luna es solo el fracaso más espectacular del sector, con muchas monedas menos conocidas que han visto un colapso en el precio de más del 90% en relación con su pico en 2021. Los comentaristas criptográficos han comenzado a referirse a los eventos recientes como el comienzo de un "invierno criptográfico".

A pesar de lo dramáticos que han sido estos recientes colapsos de precios, centrarse solo en la acción del precio desvía la atención de las fallas estructurales más profundas en las criptomonedas que las hacen inadecuadas como base para un sistema monetario que sirve a la sociedad ([Tabla 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-tab1), tercera columna).

La prevalencia de las monedas estables, que intentan vincular su valor al dólar estadounidense u otras monedas convencionales, indica la necesidad generalizada en el sector criptográfico de aprovechar la credibilidad proporcionada por la unidad de cuenta emitida por el banco central. En este sentido, las stablecoins son la manifestación de la búsqueda de criptografía de un ancla nominal. Las monedas estables se asemejan a la forma en que una paridad monetaria es un ancla nominal para el valor de una moneda nacional frente al de una moneda internacional, pero sin los arreglos institucionales, instrumentos, compromisos y credibilidad del banco central que opera la paridad. Proporcionar la unidad de cuenta para la economía es el papel principal del banco central. El hecho de que las monedas estables deben importar la credibilidad del dinero del banco central es muy revelador de las deficiencias estructurales de las criptomonedas. El hecho de que las monedas estables sean a menudo menos estables de lo que afirman sus emisores muestra que, en el mejor de los casos, son un sustituto imperfecto de una moneda soberana sólida.

Las monedas estables también desempeñan un papel clave para *facilitar las* transacciones en la gran cantidad de criptomonedas que se han multiplicado en los últimos años. En el último recuento, había más de 10,000 monedas en muchas cadenas de bloques diferentes que competían por la atención de los compradores especulativos.

La proliferación de monedas revela otro defecto estructural importante con la criptografía, a saber, la *fragmentación* del universo criptográfico, con muchas capas de asentamiento incompatibles luchando por un lugar en el centro de atención.

Esta fragmentación del universo criptográfico plantea serias preguntas sobre la idoneidad de la criptografía como dinero. El dinero es un dispositivo de coordinación que sirve a la sociedad a través de sus fuertes efectos de red. Cuantos más usuarios acudan a una forma particular de dinero, más usuarios atraerá. Por esta razón, el dinero tiene la propiedad de "el ganador se lleva todo", en la que los efectos de red conducen al dominio de una versión del dinero como el medio de transacción que generalmente se acepta en toda la economía. La fragmentación del universo criptográfico apunta en una dirección muy diferente: como se explica a continuación, cuantos más usuarios acudan a un sistema blockchain, peor es la congestión y más altas son las tarifas de transacción, abriendo la puerta a la entrada de nuevos rivales que pueden cortar esquinas en seguridad en favor de una mayor capacidad. Entonces, en lugar de la narrativa monetaria familiar de "cuanto más mejor", la criptografía muestra la propiedad de "cuanto más sórdido". Es esta tendencia a la fragmentación la que es quizás el mayor defecto de la criptografía como base para un sistema monetario.

Sin embargo, la criptografía ofrece una visión de características potencialmente útiles que podrían mejorar las capacidades del sistema monetario actual. Estos se derivan de la capacidad de combinar transacciones y ejecutar la liquidación automática de transacciones agrupadas de manera condicional, lo que permite una mayor funcionalidad y velocidad. Por lo tanto, una pregunta a considerar es cómo las funcionalidades útiles de la criptografía se pueden incorporar en un futuro sistema monetario que se basa en el dinero del banco central.

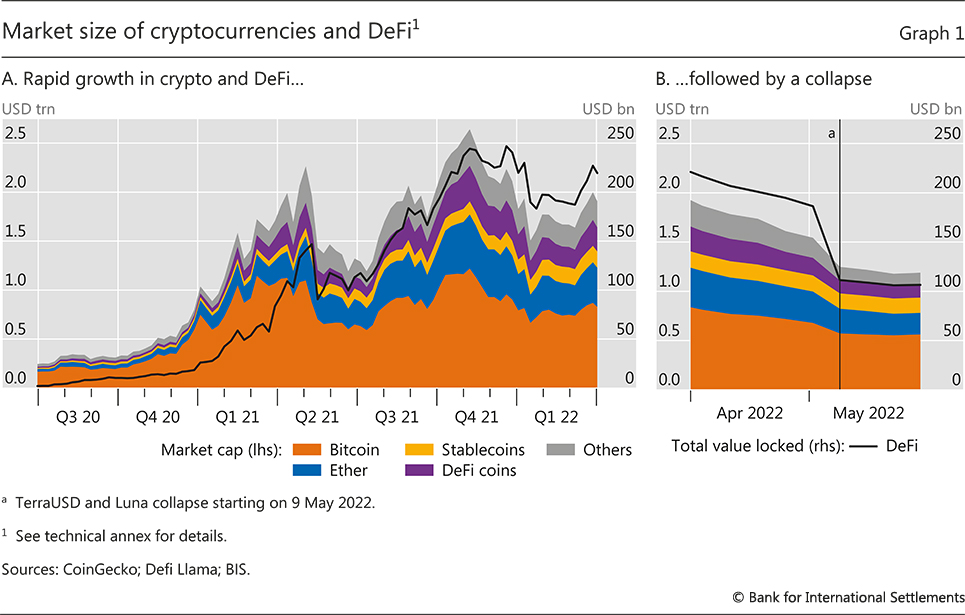
Con el fin de desarrollar los conocimientos más profundos sobre los defectos y posibilidades de la criptografía, es instructivo primero explicar algunos bloques de construcción básicos del mundo criptográfico.

**Los bloques de construcción de la criptografía**

Crypto pretende reducir el peso de los intermediarios y se ha descrito como un movimiento más amplio hacia las finanzas descentralizadas e incluso una Internet más descentralizada ("Web 3.0" o "Web3"). El beneficio promocionado es democratizar las finanzas, otorgando a los usuarios un mayor control sobre sus datos. Antes de la reciente caída, el tamaño del mercado de las criptomonedas y DeFi se había expandido rápidamente ([Gráfico 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra1)).

Crypto tiene su origen en Bitcoin, que introdujo una idea radical: un medio descentralizado de transferir valor en una cadena de bloques sin permiso. Cualquier participante puede actuar como un nodo de validación (ver glosario) y participar en la validación de transacciones en un libro mayor público (es decir, la cadena de bloques sin permiso). En lugar de depender de intermediarios de confianza (como los bancos), el mantenimiento de registros en la cadena de bloques es realizado por una multitud de validadores anónimos e interesados.

**Gráfico 1**



Las transacciones con criptomonedas son verificadas por validadores descentralizados y registradas en el libro mayor público. Si un vendedor desea transferir criptomonedas a un comprador, el comprador (cuya identidad se oculta detrás de su firma digital criptográfica) transmite los detalles de la transacción, por ejemplo, las partes de la transacción, el monto o las tarifas. Los validadores (en algunas redes llamados "mineros") compiten para verificar la transacción, y quien sea seleccionado para verificar luego agrega la transacción a la cadena de bloques. La cadena de bloques actualizada se comparte entre todos los mineros y usuarios. Por lo tanto, el historial de todas las transacciones es públicamente observable y está vinculado a billeteras específicas, mientras que las verdaderas identidades de las partes detrás de las transacciones (es decir, los propietarios de las billeteras) permanecen sin revelar. Al transmitir toda la información públicamente, el sistema verifica que la transacción sea consistente con el historial de transferencias en la cadena de bloques, es decir, que la criptomoneda realmente pertenece al vendedor y no se ha gastado dos veces.

Sin embargo, para un sistema de gobernanza descentralizado, los incentivos económicos son clave. Los límites del sistema son establecidos por las leyes de la economía en lugar de las leyes de la física. En otras palabras, no solo la tecnología sino también los incentivos deben funcionar. Los mineros (o validadores) son compensados con recompensas monetarias por realizar sus tareas de acuerdo con las reglas para que el sistema se vuelva autosuficiente. Las recompensas, pagadas en criptomonedas, pueden venir en forma de tarifas de transacción, pero también pueden provenir de alquileres que se acumulan al "apostar" las monedas de uno en una cadena de bloques de prueba de participación. Cuanto mayor sea la apuesta, más a menudo un nodo servirá como validador, y mayores serán las rentas.

Desde el advenimiento de Bitcoin en 2009, muchas otras cadenas de bloques y criptomonedas asociadas han entrado en escena, especialmente Ethereum, que prevé el uso de "contratos inteligentes" y "programabilidad" (ver glosario). Los contratos inteligentes, o código autoejecutable que desencadena una acción si se cumplen algunas condiciones preespecificadas, pueden automatizar las funciones del mercado y obviar a los intermediarios que tradicionalmente se requerían para tomar decisiones. A medida que el código subyacente está disponible públicamente, puede ser examinado, haciendo que los contratos inteligentes sean transparentes y reduciendo el riesgo de manipulación. Una característica importante de los contratos inteligentes es su componibilidad, o la capacidad de combinar diferentes componentes en un sistema. Los usuarios pueden realizar transacciones complejas en la misma cadena de bloques combinando múltiples instrucciones dentro de un solo contrato inteligente: "legos de dinero". Pueden crear una representación digital de activos a través de la "tokenización" (ver glosario). Como los contratos inteligentes no pueden acceder directamente a la información que reside "fuera de la cadena", es decir, fuera de la cadena de bloques específica, requieren que los mediadores proporcionen dichos datos (los llamados oráculos).4

Las cadenas de bloques más nuevas, con Terra (antes de su colapso) como un ejemplo prominente, se han promocionado como "asesinos de Ethereum" en el sentido de que cuentan con una mayor capacidad y un mayor rendimiento (ver glosario). Sin embargo, estos cambios traen nuevos problemas. La capacidad a menudo se incrementa a través de una mayor centralización en los mecanismos de validación, debilitando la seguridad y concentrando los beneficios para los iniciados, como se explica a continuación.5

**Stablecoins en busca de un ancla nominal**

Un desarrollo clave en el universo criptográfico es el aumento de las finanzas descentralizadas, o "DeFi". DeFi ofrece servicios y productos financieros, pero con el objetivo declarado de remodelar el sistema financiero eliminando a los intermediarios y, por lo tanto, reduciendo los costos.6 Con este fin, las aplicaciones DeFi registran públicamente transacciones pseudo-anónimas en criptomonedas en blockchains sin permiso. Las "aplicaciones descentralizadas" (dApps) con contratos inteligentes permiten automatizar las transacciones. Para llegar a un consenso, los validadores son incentivados a través de recompensas.

Si bien el ecosistema DeFi está evolucionando rápidamente, los principales tipos de actividad financiera siguen siendo los que ya están disponibles en las finanzas tradicionales, como los préstamos, el comercio y los seguros.7 Las plataformas de préstamos permiten a los usuarios prestar sus stablecoins con intereses a los prestatarios que publican otras criptomonedas como garantía. Los intercambios descentralizados (DEX) representan mercados donde las transacciones ocurren directamente entre comerciantes de criptomonedas o stablecoins, con precios determinados a través de algoritmos. En las plataformas de seguros DeFi, los usuarios pueden asegurarse contra el mal manejo de las claves privadas, los hacks de intercambio o las fallas de los contratos inteligentes. Como las actividades implican casi exclusivamente el intercambio de una stablecoin o criptomoneda por otra, y no financian inversiones productivas en la economía real, el sistema es en su mayoría autorreferencial.

Las stablecoins juegan un papel clave en el ecosistema DeFi. Estos se llaman así porque generalmente están vinculados a un numerario, como el dólar estadounidense, pero también pueden apuntar al precio de otras monedas o activos (por ejemplo, el oro). En este sentido, a menudo importan la credibilidad proporcionada por la unidad de cuenta emitida por el banco central. Su principal caso de uso es superar la alta volatilidad de los precios y la baja liquidez de las criptomonedas sin respaldo, como Bitcoin. Su uso también evita la conversión frecuente entre criptomonedas y depósitos bancarios en moneda soberana, que generalmente se asocia con tarifas significativas. Debido a que las stablecoins se utilizan para soportar una amplia gama de actividades DeFi, la rotación en stablecoins generalmente empequeñece la de otras criptomonedas.

Los dos tipos principales de stablecoin son respaldados por activos y algorítmicos. Las monedas estables respaldadas por activos, como Tether, USD Coin y Binance USD, generalmente son administradas por un intermediario centralizado que invierte la garantía subyacente y coordina el reembolso y la creación de las monedas. Los activos se pueden mantener en bonos del gobierno, deuda corporativa a corto plazo o depósitos bancarios, o en otras criptomonedas. En contraste, las monedas estables algorítmicas, como TerraUSD antes de su implosión, se basan en algoritmos complejos que reequilibran automáticamente la oferta para mantener su valor en relación con la moneda o activo objetivo. Para evitar la dependencia de la moneda fiduciaria, a menudo lo hacen proporcionando a los usuarios una oportunidad de arbitraje en relación con otra criptomoneda.

A pesar de su nombre, las stablecoins, en particular, las algorítmicas, son menos estables de lo que afirman sus emisores. En mayo de 2022, TerraUSD entró en una espiral de muerte, ya que su valor cayó de $ 1 a solo unos pocos centavos en el transcurso de unos pocos días (ver [Recuadro A](https://www.bis.org/publ/arpdf/ar2022e3.htm#box-A)). Posteriormente, otras monedas estables algorítmicas se vieron presionadas. Pero también lo hicieron algunas monedas estables respaldadas por activos, que han visto reembolsos a gran escala, perdiendo temporalmente su paridad a raíz del shock. Los reembolsos fueron más pronunciados entre las monedas estables cuyos emisores no revelaron la composición de los activos de reserva en detalle, lo que presumiblemente refleja las preocupaciones de los inversores de que dichos emisores podrían no ser capaces de garantizar la conversión a la par.

De hecho, los comentaristas han advertido durante algún tiempo que existe un conflicto de intereses inherente en las monedas estables, con un incentivo para que los emisores inviertan en activos de mayor riesgo. La historia económica está plagada de intentos de dinero privado que fracasaron, lo que llevó a pérdidas para los inversores y la economía real. La solidez de los mecanismos de estabilización de las monedas estables depende fundamentalmente de la calidad y la transparencia de sus activos de reserva, que a menudo son lamentablemente deficientes.8

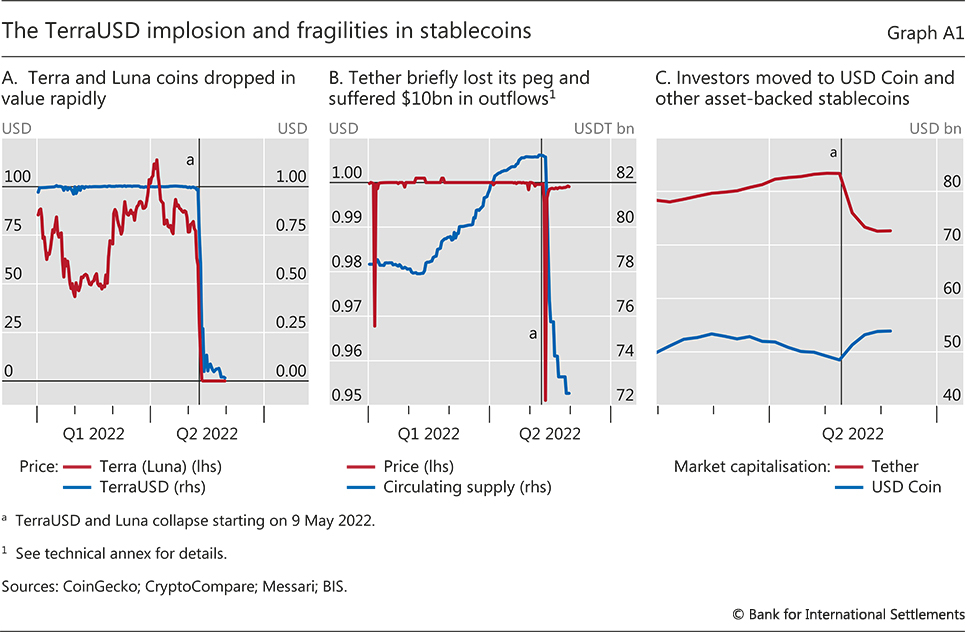
Sin embargo, incluso si las monedas estables se mantuvieran estables hasta cierto punto, carecen de las cualidades necesarias para apuntalar el futuro sistema monetario. Deben importar su credibilidad de monedas fiduciarias soberanas, pero no se benefician ni de los requisitos regulatorios y las protecciones de los depósitos bancarios y el dinero electrónico, ni del banco central como prestamista de último recurso. Además, atan la liquidez y pueden fragmentar el sistema monetario, socavando así la unicidad de la moneda.9 Como las stablecoins apenas se utilizan para pagar bienes y servicios del mundo real, pero sustentan el ecosistema DeFi en gran parte autorreferencial, algunos han cuestionado si las stablecoins deberían prohibirse.10 Como se discutirá a continuación, hay más promesas en las representaciones más sólidas del dinero del banco central y los pasivos de los emisores regulados.

**Recuadro A**

**El colapso de la stablecoin TerraUSD**

La implosión de TerraUSD (UST) destaca las fragilidades inherentes en algunas versiones de stablecoins. El uso de UST creció rápidamente durante 2021-22, por lo que, antes de su colapso, era la tercera moneda estable más grande, con una capitalización de mercado máxima de $ 18.7 mil millones. Una *stablecoin algorítmica*, mantuvo el valor ajustando la oferta en una estrategia de comercio de arbitraje automatizado con otra criptomoneda, Luna, en la cadena de bloques Terra. UST tenía como objetivo mantener una paridad uno por uno con el dólar estadounidense al ser convertible en el valor de un dólar de Luna, y viceversa. Por ejemplo, si Terra cae a 99 centavos, un usuario podría comprar UST en un intercambio por 99 centavos y luego cambiar su UST por $ 1 en unidades nuevas de Luna en la plataforma Terra. Un aspecto crucial de este acuerdo era que los usuarios solo estarían dispuestos a intercambiar UST en Luna si la capitalización de mercado de Luna excedía la de UST. Como Luna no tenía un valor intrínseco, su valoración se derivaba principalmente de la afluencia de usuarios especulativos al ecosistema terra. Para atraer a nuevos usuarios, el protocolo de préstamos asociado Anchor ofreció una tasa de depósito de alrededor del 20% en UST. Mientras los usuarios tuvieran confianza en el valor estable de UST y la capitalización de mercado sostenida de Luna, el sistema podría mantenerse. La dupla Terra/Luna fue considerada especialmente significativa, ya que prometía ofrecer una versión de dinero "autolevitante" que no se aprovechaba de los activos colaterales del mundo real.

**Gráfico A1**



Sin embargo, esta esperanza resultó infundada. Una vez que los inversores perdieron la confianza en la sostenibilidad del sistema, el acuerdo se desmoronó. En mayo de 2022, el valor de UST se desplomó a casi cero ([Gráfico A1. R](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxA-graA1)). A medida que ust cayó por debajo de su paridad, una dinámica de carrera clásica se afianzó a medida que los inversores buscaban canjear sus fondos. Los usuarios quemaron su UST a gran escala para acuñar $ 1 en luna nueva, con la esperanza de vender Luna siempre que todavía tuviera algún valor. Sin embargo, dado el tamaño y la velocidad del choque, la confianza se evaporó, lo que significa que no había suficientes partes dispuestas a comprar todas las monedas Luna recién acuñadas, por lo que el precio de Luna se derrumbó.

La implosión ust/luna se extendió a la moneda estable más grande, Tether, que cayó a un valor de $ 0.95 antes de recuperarse. Vio salidas de más de $ 10 mil millones en las semanas siguientes ([Gráfico A1. B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxA-graA1)). La desvinculación se ha relacionado con la falta de voluntad de Tether para proporcionar detalles sobre su cartera de reservas: los inversores estaban preocupados por si Tether tenía suficientes activos de alta calidad que pudieran liquidarse para respaldar la paridad. Este argumento está respaldado por las entradas experimentadas por la stablecoin regulada USDC (con reservas mejor documentadas), con fondos probablemente provenientes de Tether ([Gráfico A1. C](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxA-graA1)).

**Limitaciones estructurales de la criptografía**

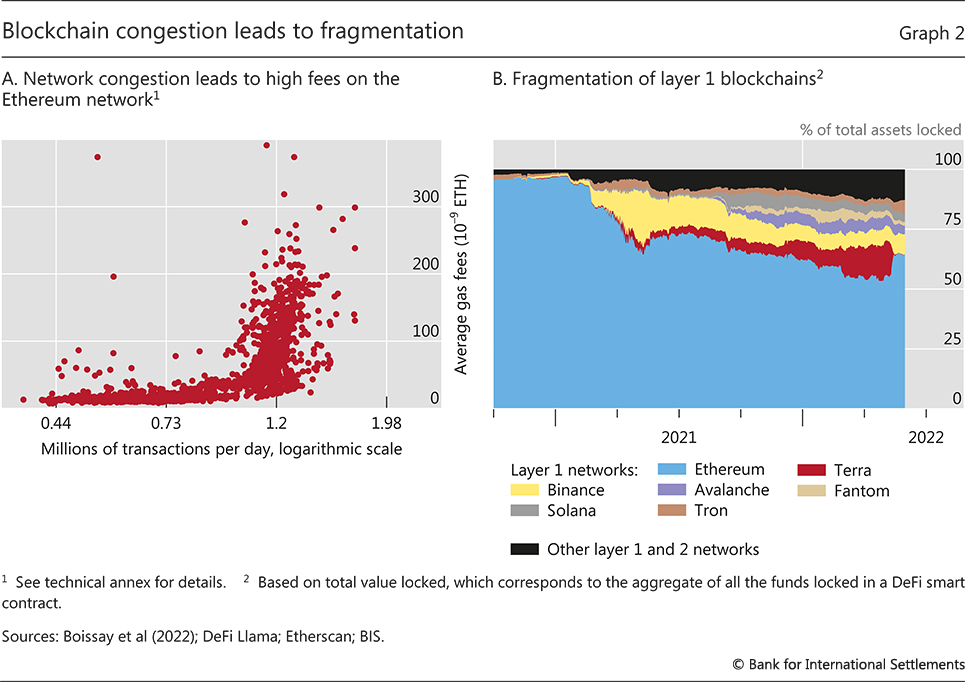
Además de las preocupaciones inmediatas en torno a la estabilidad, las criptomonedas sufren de las limitaciones inherentes de las cadenas de bloques sin permiso, que conducen inevitablemente a la fragmentación del sistema, acompañada de congestión y altas tarifas.11 Rastrear las razones de la fragmentación es revelador, ya que ponen de relieve que las limitaciones no son tecnológicas, sino que se derivan de la estructura de incentivos del sistema.

Los validadores interesados son responsables de registrar las transacciones en la cadena de bloques. Sin embargo, en el sistema criptográfico pseudo-anónimo, no tienen reputación en juego y no pueden rendir cuentas bajo la ley. En cambio, deben ser incentivados a través de recompensas monetarias que sean lo suficientemente altas como para sostener el sistema de consenso descentralizado. La validación honesta debe producir rendimientos más altos que las ganancias potenciales de hacer trampa. Si las recompensas caen demasiado bajo, los validadores individuales tendrían un incentivo para engañar y robar fondos. El mecanismo de consenso fracasaría, poniendo en peligro la seguridad general.

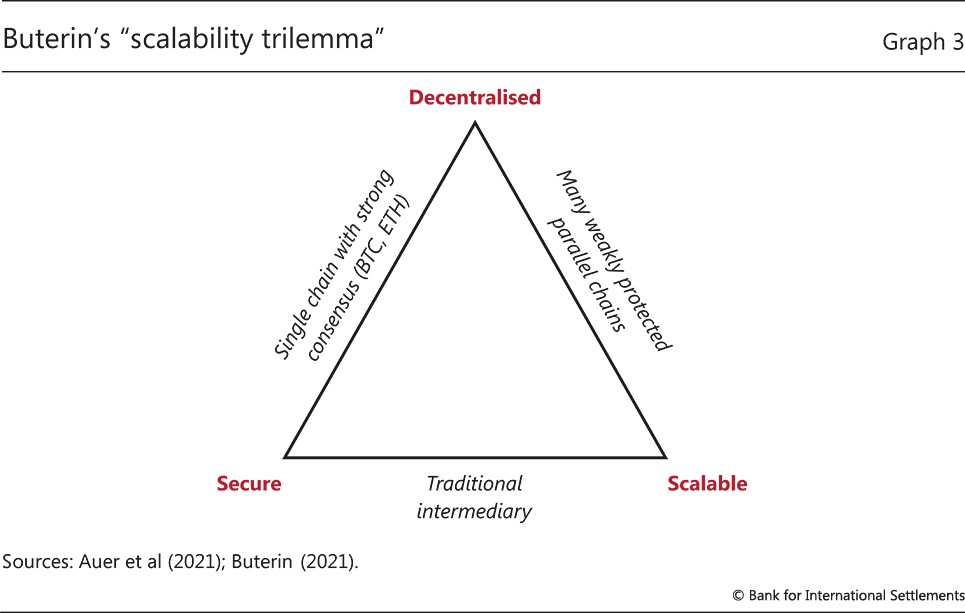
La única forma de canalizar las recompensas a los validadores, manteniendo así los incentivos, es limitar la capacidad de la cadena de bloques, manteniendo así altas las tarifas, sostenidas por la congestión. Como los validadores pueden elegir qué transacciones se validan y procesan, los períodos de congestión ven a los usuarios ofreciendo tarifas más altas para que sus transacciones se procesen más rápido ([Gráfico 2 A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra2)).12

La escala limitada de las cadenas de bloques es una manifestación del llamado trilema de escalabilidad. Por su naturaleza, las cadenas de bloques sin permiso pueden lograr solo dos de tres propiedades, a saber, escalabilidad, seguridad o descentralización ([Gráfico 3](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra3)). La seguridad se mejora a través de incentivos y descentralización, pero mantener los incentivos a través de tarifas implica congestión, lo que limita la escalabilidad. Por lo tanto, existe una incompatibilidad mutua entre estos tres atributos clave, lo que impide que las cadenas de bloques sirvan adecuadamente al interés público.

**Gráfico 2**



**Gráfico 3**



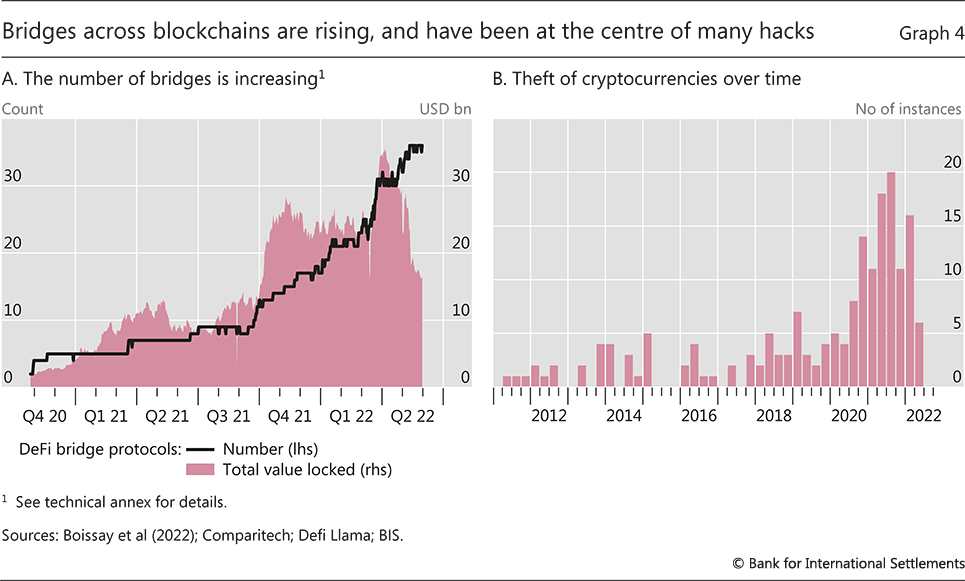
La escalabilidad limitada de las cadenas de bloques ha fragmentado el universo criptográfico, ya que las nuevas cadenas de bloques que cortan las esquinas en materia de seguridad han entrado en la refriega. La cadena de bloques Terra es solo la más prominente de una horda de nuevos participantes ([Gráfico 2.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra2)). Incluso a principios de 2021, Ethereum representó casi todos los activos totales bloqueados. A principios de mayo de 2022, esta proporción ya había caído al 50%. La cuña de ensanchamiento (en rojo) explicada por la fallida cadena de bloques Terra es particularmente llamativa. El colapso de Terra destaca la tendencia del universo criptográfico a fragmentarse a través de su vulnerabilidad a nuevos participantes que priorizan la cuota de mercado y la capacidad a expensas de la descentralización y la seguridad.

Un sistema de cadenas de bloques competidoras que no son interoperables pero sostenidas por la especulación introduce nuevos riesgos de piratería y robo. La interoperabilidad se refiere aquí a la capacidad de los protocolos y validadores para acceder y compartir información, así como validar transacciones, a través de diferentes cadenas de bloques. La interoperabilidad de las capas de liquidación subyacentes no se puede lograr en la práctica, ya que cada cadena de bloques es un registro separado de las liquidaciones. Sin embargo, han surgido "puentes de cadena cruzada" para permitir a los usuarios transferir monedas a través de blockchains.13 Sin embargo, la mayoría de los puentes dependen solo de un pequeño número de validadores, en ausencia de regulación y responsabilidad legal, los usuarios deben confiar para no participar en comportamientos ilícitos. Pero, a medida que el número de puentes ha aumentado ([Gráfico 4.A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra4)), los puentes han ocupado un lugar destacado en varios hacks de alto perfil ([Gráfico 4.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra4)). Estos ataques ponen de relieve las vulnerabilidades a las brechas de seguridad que se derivan de la debilidad en la gobernanza.

La sorprendente fragmentación del universo criptográfico contrasta con los efectos de red que se arraigan en las redes de pago tradicionales. Las redes de pago tradicionales se caracterizan por una propiedad de "el ganador se lo lleva todo", por la cual más usuarios que acuden en masa a una plataforma en particular engendran aún más usuarios. Tales efectos de red se encuentran en el corazón del círculo virtuoso de menores costos y mayor confianza en las plataformas tradicionales. En contraste, la tendencia de la criptografía hacia la fragmentación y las altas tarifas es una falla estructural fundamental que la descalifica como la base para el futuro sistema monetario.14

A pesar de la fragmentación, la especulación puede inducir altas correlaciones de precios entre diferentes criptomonedas y cadenas de bloques. Atraídos por los altos rendimientos y la expectativa de nuevos aumentos de precios ([recuadro B](https://www.bis.org/publ/arpdf/ar2022e3.htm#box-B)), la afluencia de nuevos usuarios puede hacer subir los precios aún más. Como muchas criptomonedas comparten una base de usuarios similar y están vinculadas a protocolos similares, existe un fuerte co-movimiento de precios. Hay preocupaciones importantes sobre lo que sucede con un sistema que se basa en la venta de nuevas monedas cuando la nueva afluencia de usuarios se ralentiza repentinamente.

**Gráfico 4**



**La ilusión de la descentralización DeFi y el papel de los intercambios**

A pesar de su nombre, el ecosistema DeFi muestra una tendencia hacia la centralización. Muchas decisiones clave se toman por votación entre los titulares de "tokens de gobernanza", que a menudo se emiten a los equipos de desarrolladores y a los primeros inversores y, por lo tanto, están muy concentrados. Los contratos inteligentes vinculados a eventos del mundo real involucran oráculos que operan fuera de la cadena de bloques. La "incompletitud del algoritmo", es decir, la imposibilidad de redactar contratos para detallar qué acciones tomar en todas las contingencias, requiere que algunas entidades centrales resuelvan las disputas. Además, las cadenas de bloques más nuevas generalmente apuntan a transacciones más rápidas y un mayor rendimiento al confiar en mecanismos de validación concentrados. Por ejemplo, los mecanismos de prueba de participación se basan en un número limitado de validadores que apuestan sus monedas.

La centralización en DeFi no está exenta de riesgos. La creciente centralización de los validadores da lugar a conflictos de incentivos y al riesgo de hackeos, también porque estos nodos centralizados a menudo no están regulados.15 Además, los responsables de un oráculo pueden corromper el sistema informando erróneamente los datos (el llamado problema del oráculo). Actualmente, no hay reglas claras sobre cómo examinar o incentivar a los proveedores de oracle.

La centralización también está presente en las actividades de comercio de criptomonedas, donde los inversores dependen principalmente de los intercambios centralizados (CEX) en lugar de los descentralizados (DEX). Mientras que estos últimos funcionan haciendo coincidir a las contrapartes en una transacción a través de los llamados protocolos automatizados de creación de mercado, los CÉX mantienen registros fuera de la cadena de las órdenes pendientes publicadas por los comerciantes, conocidos como libros de órdenes límite, que son familiares de las finanzas tradicionales. Los CEX atraen más actividad comercial que los DEX, ya que presentan costos más bajos ([Gráfico 5.A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra5)).16 En términos de modelo de negocio y la forma en que operan, los CEX criptográficos no son fundamentalmente diferentes de los intercambios tradicionales, a pesar de que no están sujetos a la misma regulación y supervisión.

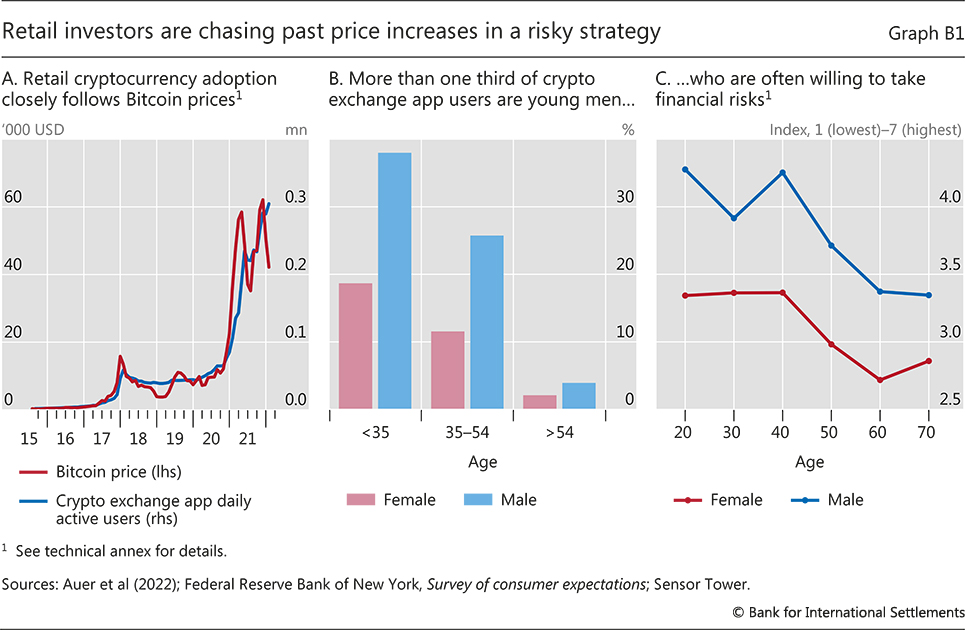
**Recuadro B**

**Comercio de criptomonedas y precios de Bitcoin**

La especulación es un impulsor clave de las tenencias de criptomonedas,[icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#b1) pero los inversores minoristas pueden no ser plenamente conscientes de los riesgos asociados con las inversiones en criptomonedas. Un estudio reciente de BIS reúne una nueva base de datos entre países sobre el uso minorista de aplicaciones de intercambio de criptomonedas con una frecuencia diaria durante 2015-22, centrándose en la relación entre el uso de aplicaciones de comercio de criptomonedas y los precios de Bitcoin. [icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#b2) El análisis muestra que una subida del precio de Bitcoin se asocia a un aumento significativo de nuevos usuarios, es decir, la entrada de nuevos inversores, con un coeficiente de correlación de más de 0,9 ([Gráfico B1. R](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxB-graB1)). Un aumento de una desviación estándar en el precio diario de Bitcoin se asocia con un aumento de alrededor de 90,000 usuarios de aplicaciones de intercambio de criptomonedas. Los usuarios de aplicaciones criptográficas son principalmente usuarios y hombres más jóvenes ([Gráfico B1.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxB-graB1)), comúnmente identificados como el segmento de la población que más "busca riesgos", y potencialmente motivados por un "miedo a perderse". Estos patrones son consistentes con la evidencia de la encuesta sobre la tolerancia al riesgo de los individuos: los hombres más jóvenes están más dispuestos que las mujeres o los encuestados varones mayores a asumir riesgos financieros ([Gráfico B1.C](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxB-graB1)).

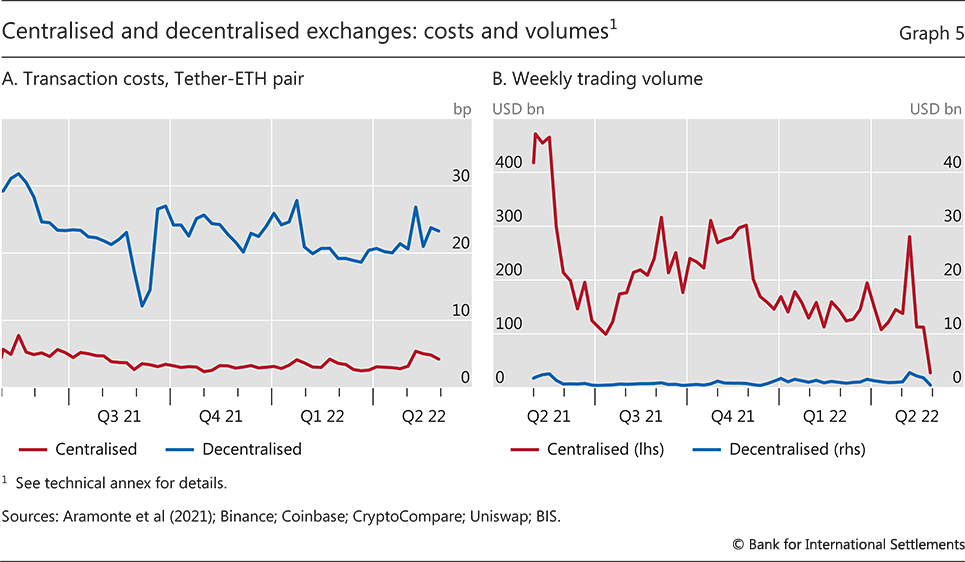
Cuantificar el efecto de los precios de Bitcoin en la entrada en criptografía es difícil debido a la posibilidad de causalidad inversa. Los precios también podrían aumentar debido a la entrada de nuevos usuarios de aplicaciones de intercambio de criptomonedas. Para abordar tales preocupaciones, es posible centrarse en choques exógenos específicos cuando los cambios en los precios de Bitcoin se debieron a factores específicos, como la represión de las autoridades chinas contra las actividades de criptominería y el malestar social en Kazajstán. Durante cada uno de estos episodios, los cambios estructurales afectaron el precio global de Bitcoin, independientemente de la entrada de nuevos usuarios en las aplicaciones de intercambio de criptomonedas. En estos casos, la caída exógena en el precio de Bitcoin se asoció con una reducción promedio en el número de nuevos usuarios de aplicaciones del 5-10% en las dos semanas posteriores a los shocks. Los resultados se corroboran aún más a partir de un modelo de autorregresión de vectores de panel, donde un aumento del 10% en el precio de Bitcoin conduce a un aumento del 3% en el número de usuarios de la aplicación.

**Gráfico B1**



[icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#a1) Las personas invierten en criptomonedas por diferentes razones, por ejemplo, porque desconfían de las instituciones financieras nacionales, por transferencias de dinero transfronterizas o por el potencial de pseudoanonimismo, ya sea por razones legítimas o nefastas. Sin embargo, una de las principales razones es que las criptomonedas son vistas como activos de inversión. Véase Auer y Tercero-Lucas (2021), Foley et al (2019), Hileman (2015), Knittel et al (2019) y Swartz (2020). [icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#a2) Auer, Cornelli, Doerr, Frost y Gambacorta (2022)

**Gráfico 5**



Los CEX han experimentado un crecimiento sustancial desde 2020 y han alcanzado volúmenes que los hacen relevantes desde el punto de vista de la estabilidad financiera ([Gráfico 5.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra5)). Además, el comercio en CEX muestra una fuerte tendencia hacia la concentración del mercado: los volúmenes de negociación en tres grandes CEX representaron alrededor de la mitad del total en los primeros meses de 2022. Sin embargo, generalmente es difícil medir el tamaño real de los intercambios de criptomonedas, porque los CEX tienen una parte significativa de sus criptomonedas de custodia fuera de balance. Por ejemplo, la plataforma Coinbase informó públicamente que tenía $ 256 mil millones de activos en la plataforma (a fines de marzo de 2022), pero un balance de solo $ 21 mil millones a fines de 2021. El personal de la Comisión de Bolsa y Valores argumentó recientemente que la plataforma debería informar tanto los pasivos (obligaciones con los clientes) como los activos en su balance.17 Además, los proveedores de servicios criptográficos a menudo realizan una multitud de servicios, lo que plantea la cuestión de si las actividades están adecuadamente delimitadas y los riesgos se gestionan adecuadamente. Por ejemplo, junto con el comercio de terceros, realizan operaciones de propiedad, préstamos de margen o emisión de tokens, y suministran servicios de custodia. A menudo, las transacciones implican interacciones entre los contratos inteligentes en cadena y las plataformas de negociación centralizadas fuera de la cadena, con la naturaleza distribuida de la liquidación en cadena que da lugar a riesgos distintos en comparación con los derivados de los operadores de infraestructura tradicionales.

Una evaluación equilibrada de las similitudes y diferencias entre el criptomercado y las finanzas tradicionales es un requisito previo para considerar políticas regulatorias apropiadas. Algunas actividades de los proveedores de servicios criptográficos también son características comunes en los bancos, aunque su combinación en una entidad no es actualmente común en las finanzas tradicionales. Además, las diferencias en las tecnologías subyacentes significan que las características y los impulsores del riesgo podrían diferir entre las finanzas tradicionales y el ecosistema criptográfico.

**Enfoques regulatorios para los riesgos criptográficos**

Se necesita una acción regulatoria para abordar los riesgos inmediatos en el sistema criptomonetario y para apoyar los objetivos de política pública.

Sobre todo, las autoridades deben abordar rigurosamente los casos de arbitraje regulatorio. Partiendo del principio de "misma actividad, mismo riesgo, mismas reglas", deben garantizar que las actividades criptográficas y DeFi cumplan con los requisitos legales para actividades tradicionales comparables. Los emisores de stablecoins, por ejemplo, se parecen a los tomadores de depósitos o a los fondos del mercado monetario (FMM). Como tal, se necesita legislación para calificar estas actividades y garantizar que estén sujetas a una regulación y divulgación prudenciales sólidas. Para los emisores de stablecoins de importancia sistémica, debe haber una supervisión sólida. Cuando las monedas estables son emitidas por grandes entidades con extensas redes y datos de usuarios, se necesitarán requisitos basados en entidades.18 El reciente colapso de la moneda estable Terra UST ha puesto de relieve la urgencia del asunto.

En segundo lugar, se necesitan políticas para apoyar la seguridad y la integridad de los sistemas monetario y financiero. Los intercambios de criptomonedas que ocultan la identidad de las partes que realizan transacciones y no cumplen con los requisitos básicos de conocimiento de su cliente (KYC) y otros requisitos del Grupo de Acción Financiera Internacional (GAFI) deben ser multados o cerrados. De lo contrario, pueden usarse para lavar dinero, evadir impuestos o financiar el terrorismo, y para eludir las sanciones económicas. Del mismo modo, los bancos, las compañías de tarjetas de crédito y otras instituciones financieras que proporcionan puntos de entrada y salida entre DeFi y el sistema tradicional deben requerir la identificación de los usuarios y realizar el cumplimiento de KYC.

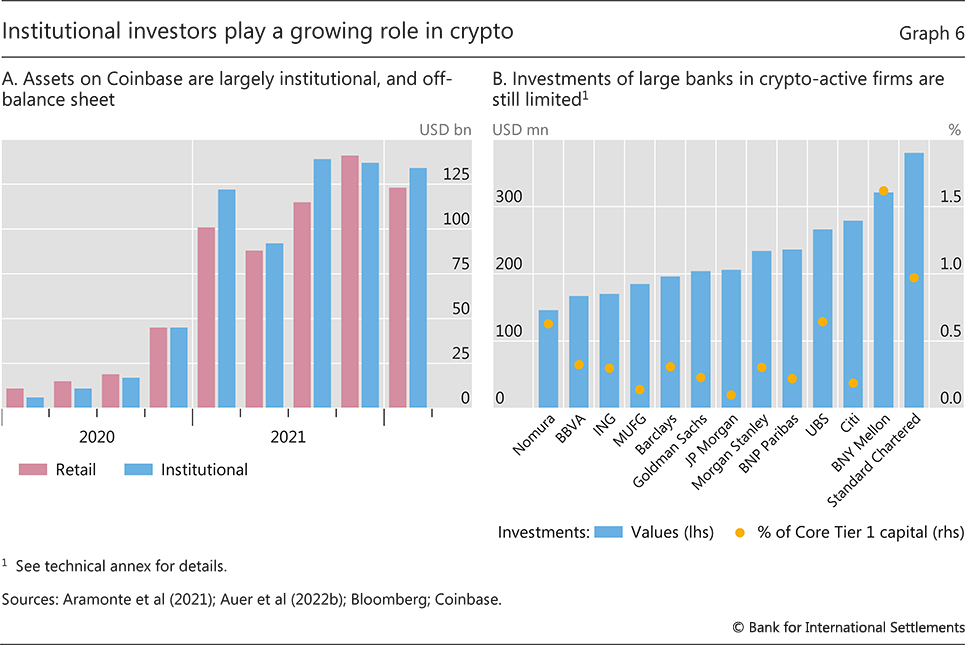
En tercer lugar están las políticas para proteger a los consumidores. Si bien se debe permitir a los inversores invertir en activos de riesgo, incluidas las criptomonedas, debe haber una divulgación adecuada. Esto implica una regulación sólida de la publicidad de activos digitales por parte de las plataformas criptográficas, que a menudo pueden ser engañosas y minimizar los riesgos. Las prácticas similares a la ejecución anticipada pueden requerir el despliegue de nuevos enfoques legales.19 Además, las plataformas descentralizadas no pueden, por diseño, asumir responsabilidad en caso de fraude o robo conectado a la plataforma, por ejemplo, como resultado de hackeos. Esto se interpone en el camino de proporcionar incentivos para la divulgación básica de los riesgos y, como tal, pueden ser necesarios nuevos enfoques.20 Esta lógica también se extiende al problema del oráculo. Las normas reglamentarias sólidas deben garantizar que no se manipule la información externa.

Finalmente, los bancos centrales y los reguladores deben mitigar los riesgos para la estabilidad financiera que surgen de la exposición de los bancos y los intermediarios financieros no bancarios al espacio criptográfico. Las inversiones de rápido crecimiento en criptomonedas por parte de las instituciones financieras tradicionales significan que los shocks en el sistema criptográfico podrían tener efectos de contagio. Según los informes, los inversores no bancarios, las oficinas familiares y los fondos de cobertura han sido los inversores institucionales más activos en criptomonedas ([Gráfico 6.A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra6)). Hasta ahora, las exposiciones de los grandes bancos tradicionales han sido limitadas y las inversiones directas en empresas activas en criptomercados siguen siendo pequeñas en relación con el capital bancario ([gráfico 6.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra6)).21 Dicho esto, la financiación bancaria de los emisores de stablecoins ha aumentado, ya que los pasivos bancarios, como los certificados de depósito, forman una parte clave del respaldo de activos de las stablecoins.22 Abordar estos riesgos implica una implementación sólida de estándares para la exposición bancaria a las criptomonedas, que deben tratar de garantizar una resistencia adecuada a los cambios grandes y repentinos en los precios o grandes pérdidas a través de canales directos e indirectos.23 Esto también puede requerir una regulación prudencial de los intercambios de criptomonedas, los emisores de monedas estables y otras entidades clave en el sistema criptográfico. Esto no excluye un enfoque innovador; por ejemplo, la supervisión podría integrarse en estos mercados, de modo que se lleve a cabo "en cadena".

Es esencial llenar las brechas de datos e identificar puntos de entrada para la regulación. El crecimiento del mercado criptográfico ha llevado a la proliferación de nuevos intermediarios centralizados. Entidades adicionales, como administradores de reservas y administradores de redes, se han desarrollado directamente como respuesta al crecimiento de las monedas estables. Estas entidades centralizadas e instituciones financieras tradicionales proporcionan una puerta de entrada natural para las respuestas regulatorias. Estas entidades también podrían apoyar la recopilación de datos mejores y más detallados sobre las actividades de DeFi, así como la base de inversores.

En todas las áreas de regulación, la naturaleza global de crypto y DeFi requerirá cooperación internacional. Es posible que las autoridades deban intercambiar información activamente y adoptar medidas conjuntas de aplicación de la ley contra los agentes y plataformas que no cumplen las normas. En algunos casos, pueden ser necesarios nuevos organismos, como colegios de supervisores, para coordinar la política hacia las mismas entidades reguladas que operan en diferentes jurisdicciones.

**Gráfico 6**



El BPI está contribuyendo a esta cooperación internacional a través de discusiones en comités del BPI como el Comité de Pagos e Infraestructuras de Mercado del BIS (BIS CPMI) y el Comité de Supervisión Bancaria de Basilea (BCBS). El BIS participa activamente en la discusión del G20 sobre la regulación de las criptomonedas, según lo coordinado por el Consejo de Estabilidad Financiera (FSB). El BPI también está desarrollando capacidades tecnológicas aplicadas en esta área para informar el diálogo internacional sobre políticas. El Centro del Eurosistema del Bis Innovation Hub está desarrollando una plataforma de análisis de criptomonedas y DeFi que combina datos dentro y fuera de la cadena para producir información examinada sobre capitalizaciones de mercado, actividad económica y flujos internacionales.

**Lecciones de Crypto para el sistema monetario**

En general, el sector criptográfico ofrece una visión de las posibilidades tecnológicas prometedoras, pero no puede cumplir con todos los objetivos de alto nivel de un sistema monetario digital. Adolece de deficiencias inherentes en estabilidad, eficiencia, responsabilidad e integridad que solo pueden abordarse parcialmente mediante la regulación. Fundamentalmente, las criptomonedas y las monedas estables conducen a un sistema monetario fragmentado y frágil. Es importante destacar que estos defectos se derivan de la economía subyacente de los incentivos, no de las restricciones tecnológicas. Y, no menos significativamente, estas fallas persistirían incluso si la regulación y la supervisión abordaran los problemas de inestabilidad financiera y el riesgo de pérdida implícito en las criptomonedas.

La tarea no es solo habilitar funciones útiles como la programabilidad, la compatibilidad y la tokenización, sino también fundamentarlas en bases más seguras para aprovechar el círculo virtuoso de los efectos de red. Los bancos centrales pueden proporcionar tales bases, y están trabajando activamente para dar forma al futuro del sistema monetario. Para servir al interés público, los bancos centrales están recurriendo a los mejores elementos de las nuevas tecnologías, junto con sus esfuerzos para regular el universo criptográfico y abordar sus inconvenientes más inmediatos.

**Visión para el futuro sistema monetario**

El futuro sistema monetario debería combinar nuevas capacidades tecnológicas con una representación superior del dinero del banco central en su núcleo. Arraigadas en la confianza en la moneda, las ventajas de las nuevas tecnologías digitales se pueden cosechar a través de la interoperabilidad y los efectos de red. Esto permite que los nuevos sistemas de pago escalen y sirvan a la economía real. De este modo, el sistema puede adaptarse a las nuevas demandas a medida que surgen, al tiempo que garantiza la unificación del dinero en actividades nuevas e innovadoras.

Los bancos centrales están en una posición única para proporcionar el núcleo del futuro sistema monetario, ya que una de sus funciones fundamentales es emitir dinero del banco central (M0), que sirve como unidad de cuenta en la economía. De la promesa básica encarnada en la unidad de cuenta, todas las demás promesas en la economía siguen.

El segundo papel fundamental del banco central, basándose en el primero, es proporcionar los medios para la finalidad última de los pagos mediante el uso de su balance. El banco central es el intermediario de confianza que debita la cuenta del pagador final y acredita la cuenta del beneficiario final. Una vez que las cuentas son debitadas y acreditadas de esta manera, el pago es definitivo e irrevocable.

La tercera función del banco central es apoyar el buen funcionamiento del sistema de pagos proporcionando suficiente liquidez para la liquidación. Dicha provisión de liquidez garantiza que ningún atasco impida el funcionamiento del sistema de pago cuando un pago se retrase porque el remitente está esperando los fondos entrantes.

El cuarto papel del banco central es salvaguardar la integridad del sistema de pagos a través de la regulación, supervisión y supervisión. Muchos bancos centrales también tienen un papel en la supervisión y regulación de los bancos comerciales y otros participantes centrales del sistema de pago. Estas funciones entrelazadas del banco central lo dejan bien situado para proporcionar la base para servicios innovadores del sector privado.24

El futuro sistema monetario se basa en estos roles del banco central para dar un margen completo a las nuevas capacidades del dinero del banco central y los servicios innovadores construidos sobre ellos. Las nuevas aplicaciones privadas podrán ejecutarse no en stablecoins, sino en representaciones tecnológicas superiores de M0, como CBDC mayoristas y minoristas, y a través de FPS minoristas que se asientan en el balance del banco central. De este modo, las innovaciones de los bancos centrales pueden apoyar una amplia gama de nuevas actividades. Debido a que los bancos centrales tienen el mandato de servir al interés público, pueden diseñar infraestructuras públicas para apoyar los objetivos de política de alto nivel del sistema monetario ([Tabla 1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-tab1), columna final) desde cero.

Esta visión implica una serie de componentes que requieren tanto definiciones formales como ejemplos. La sección primero presenta y explica estos componentes. A continuación, da una metáfora de cómo será el sistema futuro, tanto a nivel nacional como transfronterizo. Finalmente, se sumerge en los detalles de las reformas al dinero de los bancos centrales a nivel mayorista, minorista y transfronterizo, antes de revisar la posición de los bancos centrales para lograr esta visión.

**Componentes del futuro sistema monetario**

El futuro sistema monetario se basa en la división de roles probada y confiable entre el banco central, que proporciona las bases del sistema, y las entidades del sector privado que realizan las actividades orientadas al cliente. Además de esta división tradicional del trabajo, vienen nuevos estándares como las interfaces de programación de aplicaciones (API, consulte el glosario) que mejoran en gran medida la interoperabilidad de los servicios y los efectos de red asociados. No menos importante son las nuevas capacidades técnicas que abarcan la programabilidad, la componibilidad y la tokenización, que hasta ahora se han asociado con el universo criptográfico.

Esta visión contiene componentes tanto a nivel mayorista como minorista, que permiten una serie de nuevas características (en negrita).

A nivel mayorista, las monedas digitales del banco central (CBDC) pueden ofrecer nuevas capacidades y permitir transacciones entre intermediarios financieros que van más allá del medio tradicional de las reservas del banco central. Las CBDC al por mayor que se realizan transacciones utilizando tecnología de contabilidad distribuida (DLT) autorizada ofrecen **programabilidad** y liquidación atómica, de modo que las transacciones se ejecutan automáticamente cuando se cumplen las condiciones establecidas. Permiten combinar y ejecutar una serie de funciones diferentes, facilitando así la **componibilidad** de las transacciones. Estas nuevas capacidades no solo permiten la expansión de los tipos de transacciones, sino que también permiten transacciones entre una **gama mucho más amplia de intermediarios financieros**, no solo bancos comerciales. Las CBDC mayoristas también trabajan juntas a través de las fronteras, a través **de acuerdos multi-CBDC** que involucran a múltiples bancos centrales y monedas.

Dentro de las nuevas funciones desbloqueadas por las CBDC mayoristas, merece una mención especial un conjunto de aplicaciones, a saber, las derivadas de la **tokenización** de depósitos (M1) y otras formas de dinero que están representadas en redes DLT autorizadas.25 El papel de los intermediarios en la liquidación de transacciones fue uno de los principales avances en la historia del dinero, que se remonta al papel de los bancos de depósitos públicos en Europa en la historia temprana de la banca central.26 Los depósitos bancarios sirven como medio de pago, ya que el intermediario debita la cuenta del pagador y acredita la cuenta del receptor. La tokenización de depósitos toma este principio y traduce la operación a DLT creando una representación digital de los depósitos en la plataforma DLT, y liquidándolos de manera descentralizada. Esto podría facilitar nuevas formas de intercambio, incluida la propiedad fraccionada de valores y activos reales, lo que permitiría servicios financieros innovadores que se extiendan mucho más allá de los pagos.

A nivel de cara al cliente, o "minorista", las capacidades mejoradas de los intermediarios financieros benefician a los usuarios en forma de una mejor **interoperabilidad** entre las plataformas orientadas al cliente proporcionadas por los intermediarios. El núcleo de esta interoperabilidad son las API, a través de las cuales los usuarios de una plataforma pueden comunicarse fácilmente y enviar instrucciones a otras plataformas interconectadas. De esta manera, las innovaciones a nivel minorista promueven una mayor competencia, menores costos y una mayor inclusión financiera.

Concretamente, los FPS minoristas y las CBDC minoristas constituyen otra característica central del futuro sistema monetario. Los FPS minoristas son sistemas en los que la transmisión de un mensaje de pago y la disponibilidad de fondos finales al beneficiario se producen en tiempo (casi) real, en o tan cerca de las 24 horas del día, los 7 días de la semana. Muchos son operados por el banco central. Las CBDC minoristas son un tipo de CBDC a la que los hogares y las empresas pueden acceder directamente. Tanto las CBDC minoristas como los FPS permiten **pagos instantáneos** entre usuarios finales, a través de una gama de interfaces y PSP privados de la competencia. Por lo tanto, se basan en el sistema de dos niveles del banco central y los PSP privados. Las CBDC minoristas y los FPS comparten una serie de características clave adicionales y, por lo tanto, pueden considerarse como un continuo. Ambos están respaldados por una **arquitectura de datos** con identificación digital y API que permiten un intercambio seguro de datos, lo que admite un mayor control del usuario sobre los datos financieros. Al proporcionar una **plataforma abierta**, promueven la eficiencia y una mayor competencia entre los PSP del sector privado, facilitando así menores costos en los servicios de pago. A través de características de **diseño inclusivo**, ambos pueden apoyar la inclusión financiera para los usuarios que actualmente no tienen acceso a pagos digitales.

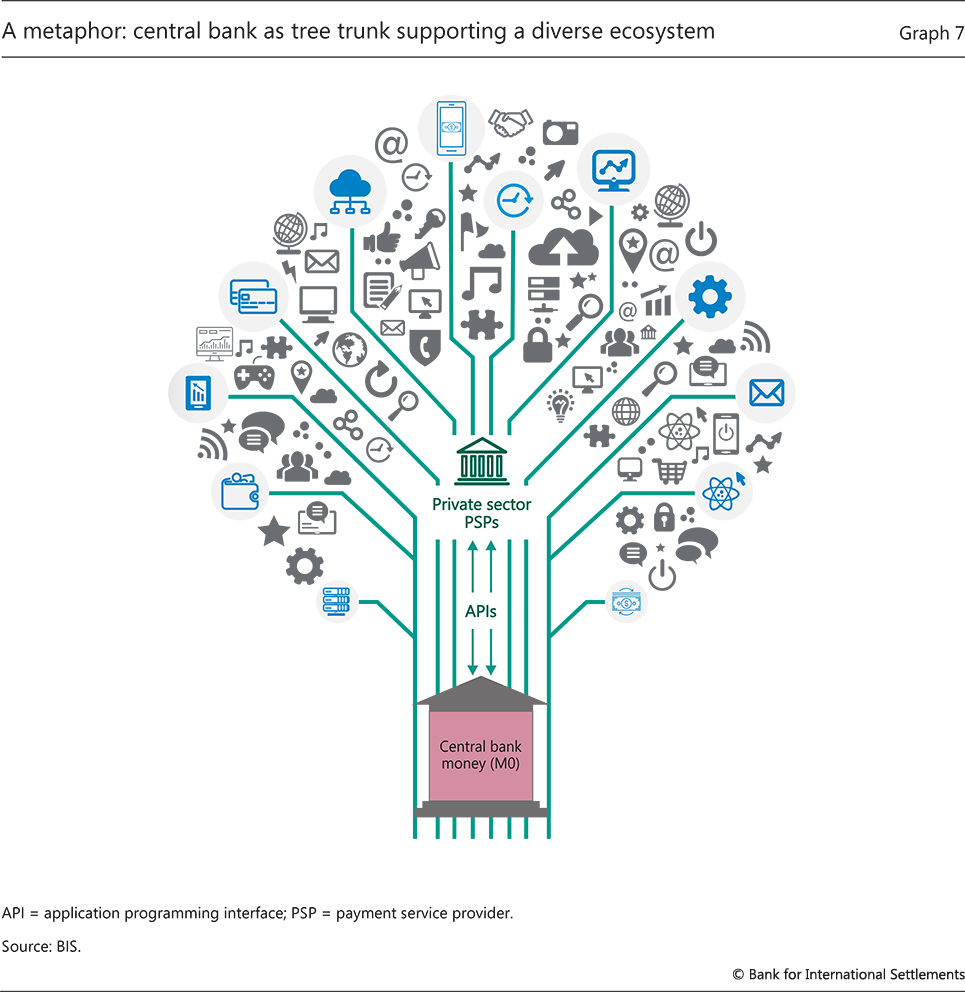
Los detalles de los componentes mayoristas y minoristas se amplían a continuación. Para cada uno de estos, una representación avanzada del dinero del banco central apoya los servicios del sector privado que sirven a la economía real. El banco central apoya la unicidad de la moneda y la interoperabilidad: la capacidad de los participantes para realizar transacciones en diferentes sistemas sin tener que participar en cada uno.27 Esto permite que los efectos de red se arraiguen, por lo que el uso de un servicio por una de las partes lo hace más atractivo para los demás.

**Una metáfora del futuro sistema monetario**

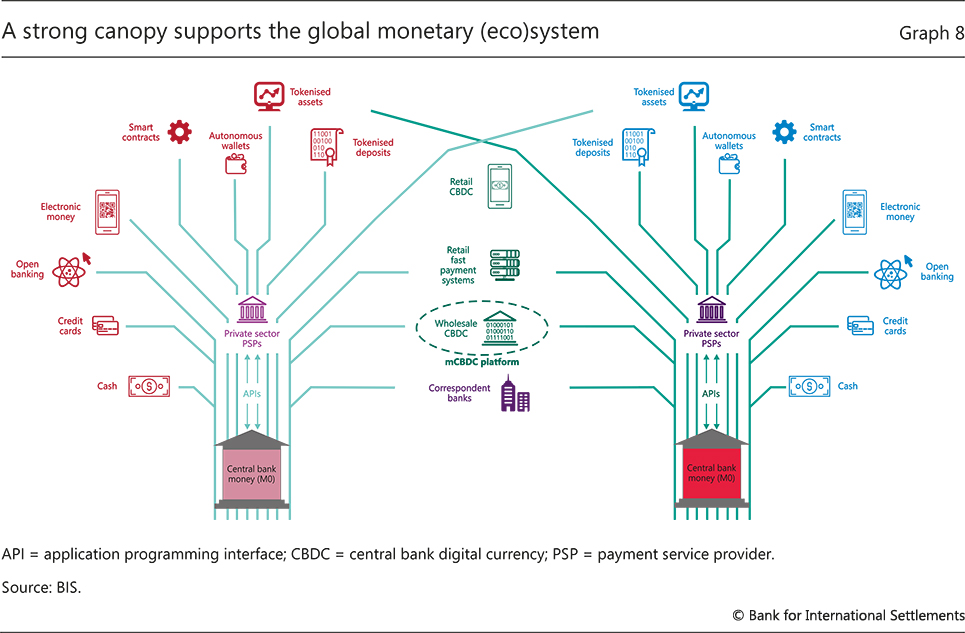
La metáfora del futuro sistema monetario es un árbol cuyo tronco sólido es el banco central ([Gráfico 7](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra7)). Además de ejemplificar el sólido apoyo proporcionado por el dinero del banco central, la metáfora del árbol expresa el principio de que el sistema monetario está arraigado (en sentido figurado) en la finalidad del pago a través de la liquidación final en el balance del banco central.

El sistema monetario basado en el dinero del banco central apoya un ecosistema vibrante diverso y de múltiples capas de participantes y funciones en el que los PSP del sector privado que compiten pueden aprovechar al máximo su creatividad e ingenio para servir mejor a los usuarios. Detrás de estos beneficios se encuentra el círculo virtuoso desencadenado por los efectos de red derivados de la arquitectura de datos, que consiste en identidad digital y API, que permite la interoperabilidad tanto a nivel nacional como transfronterizo.

**Gráfico 7**



**Gráfico 8**



Alejándose, el sistema monetario global puede compararse con un bosque, cuyo dosel facilita la actividad transfronteriza y transmonetaria ([Gráfico 8](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra8)). En el dosel, las infraestructuras como las plataformas multi-CBDC sirven como nuevos elementos importantes del sistema, como se discute en detalle a continuación. La funcionalidad de las nuevas plataformas en el dosel está en última instancia arraigada en las capas de asentamiento doméstico debajo.

La innovación no se trata solo de la última moda o palabra de moda. Así como un árbol no puede sostener un ecosistema vibrante sin un tronco sólido, obtener lo básico correcto es un requisito previo para la innovación privada que sirve al interés público. El trabajo en curso en los bancos centrales está mostrando cómo las infraestructuras públicas pueden mejorar el sistema de pago, aprovechando muchos de los supuestos beneficios de la criptografía sin los inconvenientes. Las CBDC mayoristas y minoristas, los FPS y otras reformas en la banca abierta muestran cómo los bancos centrales pueden apoyar la interoperabilidad y la gobernanza de los datos. En el cumplimiento de sus mandatos de interés público, los bancos centrales no están trabajando solos, sino que colaboran estrechamente con otras autoridades públicas e innovadores del sector privado. Las siguientes subsecciones completan los detalles de cómo funciona el sistema, junto con ejemplos concretos de las funcionalidades.

**CBDC al por mayor y dinero tokenizado**

Una CBDC es un instrumento de pago digital, denominado en la unidad de cuenta nacional, que es un pasivo directo del banco central.28 Mucha atención se ha centrado recientemente en las CBDC minoristas que son accesibles para los hogares y las empresas (se analizan a continuación). Sin embargo, las CBDC al por mayor también ofrecen nuevas funciones para el pago y la liquidación, y a una gama mucho más amplia de intermediarios que los bancos comerciales nacionales. Podrían desbloquear una importante innovación del sector privado en una amplia gama de servicios financieros.

Las CBDC al por mayor pueden permitir a los intermediarios acceder a nuevas capacidades que no son proporcionadas por las reservas mantenidas por los bancos comerciales con el banco central. Estos son particularmente relevantes en las redes DLT autorizadas, donde una red descentralizada de participantes de confianza accede a un libro mayor compartido. Como se discute a continuación, la gobernanza descentralizada es una característica útil de los sistemas multi-CBDC que involucran a múltiples bancos centrales y monedas. Sin embargo, las funciones podrían, en principio, ofrecerse en sistemas de pago más centralizados. La clave son los contratos inteligentes autoejecutables que permiten a los participantes hacer que sus transacciones sean programables. Por lo tanto, las transacciones se liquidan solo cuando se cumplen ciertas condiciones preespecificadas. En el comercio de seguridad, dicha automatización puede permitir mecanismos de pago vs pago (PvP) y entrega vs pago (DvP), lo que significa que los pagos y la entrega de un valor se realizan solo todos juntos o no se realizan en absoluto. Dicha liquidación atómica puede acelerar significativamente la liquidación y mitigar el riesgo de contraparte.29

Uno de los beneficios de las CBDC al por mayor es que podrían estar disponibles para una gama mucho más amplia de intermediarios que solo los bancos comerciales nacionales. Permitir que los PSP no bancarios realicen transacciones en CBDC podría generar una competencia y vitalidad mucho mayores. Los nuevos protocolos basados en CBDC al por mayor podrían ser de código abierto, haciendo que el código fuente esté disponible gratuitamente para que una comunidad de desarrolladores lo desarrolle y examine. Esta característica permitiría bibliotecas de protocolos que se pueden utilizar para combinar funciones, facilitando así la componibilidad de diferentes funciones y permitiendo que se construyan nuevos servicios sobre la función de programabilidad de las CBDC.

Por construcción, las CBDC al por mayor permitirían la finalidad en los pagos. La mecánica de cómo se alcanza la finalidad en las plataformas DLT autorizadas se describe con más detalle en [el recuadro C](https://www.bis.org/publ/arpdf/ar2022e3.htm#box-C), pero su esencia se puede explicar a través de la simple analogía con un billete físico. El destinatario de un billete físico quiere estar seguro de que el billete es genuino, no falso. Asegurar que el pago es en dinero genuino en un sistema digital se logra probando el origen o "procedencia" del dinero transferido. Crypto demuestra su procedencia al publicar públicamente el historial completo de todas las transacciones de todos. Cuando se usan nombres reales, dicha publicación pública violaría la privacidad y no sería adecuada como sistema de pago. Aquí es donde las técnicas criptográficas como las pruebas de conocimiento cero (ZKPs) proporcionan una solución. Como su nombre lo indica, "prueba" denota que una afirmación es verdadera, y "conocimiento cero" significa que no se expone información adicional más allá de la validez de la afirmación. Las técnicas criptográficas permiten al pagador probar que el dinero se obtuvo de transacciones pasadas válidas sin tener que publicar el historial completo de todas las transacciones. Dependiendo de la implementación detallada, es posible que se necesite un "notario" para evitar que el mismo token digital se gaste dos veces; en muchos casos, el banco central puede desempeñar este papel. El tema común es que la descentralización se puede lograr sin los defectos estructurales de la criptografía.

Como emisores de la moneda de liquidación, los bancos centrales pueden apoyar la tokenización de instrumentos financieros regulados, como los depósitos minoristas.30 Los depósitos tokenizados son una representación digital de los depósitos de los bancos comerciales en una plataforma DLT. Representarían un reclamo sobre el banco comercial del depositante, tal como lo hace un depósito regular, y serían convertibles en dinero del banco central (ya sea en efectivo o CBDC minorista) a su valor nominal. Los depositantes podrían convertir sus depósitos dentro y fuera de tokens, e intercambiarlos por bienes, servicios u otros activos. Los depósitos tokenizados también estarían protegidos por el seguro de depósitos, pero, a diferencia de los depósitos tradicionales, también serían programables y "siempre activos" (24/7), prestándose así a usos más amplios en pagos minoristas, por ejemplo, en ecosistemas autónomos. De esta manera, podrían facilitar la tokenización de otros activos financieros, como acciones o bonos. Esta funcionalidad podría permitir la propiedad fraccionada de activos y la capacidad de intercambiarlos las 24 horas del día, los 7 días de la semana. Crucialmente, esto podría hacerse en un sistema regulado, con asentamientos en CBDC al por mayor.

**Recuadro C**

**Hacer uso de DLT con dinero del banco central**

En una cadena de bloques sin permiso utilizada para aplicaciones criptográficas, todas las transacciones son públicas. La privacidad se mantiene ocultando la identidad real del usuario detrás de una clave privada. En este sentido, existe *el pseudoanonimismo*. [icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#d1) Por el contrario, un sistema monetario basado en los nombres reales de los usuarios plantea la cuestión de cómo salvaguardar su privacidad. La privacidad tiene los atributos de un derecho humano fundamental. Nadie más necesita saber en qué supermercado compra un individuo sus comestibles. Por lo tanto, una tarea básica de un sistema monetario descentralizado basado en nombres reales es encontrar una manera de garantizar que el libro mayor sea seguro sin la necesidad de una autoridad central, al mismo tiempo que se preserva la privacidad de las transacciones individuales.

Una ruta posible es a través de sistemas DLT autorizados. En estos sistemas, solo los usuarios seleccionados que cumplan con los requisitos de elegibilidad pueden obtener acceso. Por lo tanto, las interacciones entre los participantes del sistema son invisibles para las personas fuera del sistema. Un ejemplo es el sistema DLT autorizado Corda, que es utilizado por instituciones financieras privadas (por ejemplo, para plataformas de financiamiento comercial) y en una serie de proyectos mayoristas de CBDC del banco central, incluidos los Proyectos Helvetia, Jura y Dunbar en el Centro de Innovación bis.

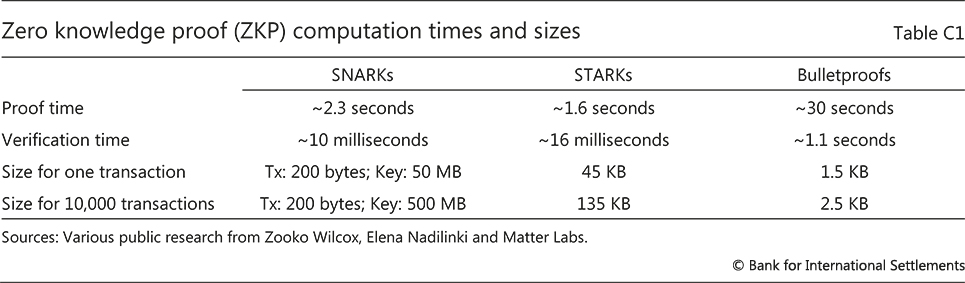
En Corda, las actualizaciones del libro mayor se realizan a través de una función de validación y una función de unicidad. La validación, que consiste en comprobar que los detalles de la transacción son correctos y que el remitente tiene los fondos disponibles, es realizada por los participantes del sistema. De hecho, solo los participantes que están involucrados en una transacción son responsables de validarla. Sin embargo, verificar que el remitente tenga un reclamo válido de fondos no garantiza que no intentará gastar esos mismos fondos dos veces. La singularidad de la transacción (es decir, la prevención del doble gasto) está garantizada por una autoridad centralizada llamada "notario". Los notarios tienen acceso a todo el libro mayor y, por lo tanto, pueden asegurarse de que los fondos que se utilizan en una transacción en particular no se utilicen en otro lugar. En el caso de las CBDC mayoristas, un candidato natural para el notario es el banco central, ya que esta institución ya desempeña un papel similar en el mantenimiento de la integridad del registro general de transacciones en sistemas centralizados.

En tales sistemas autorizados, puede surgir una tensión entre la integridad del pago y la privacidad transaccional. La privacidad transaccional en un intercambio de igual a igual significa que solo los dos participantes involucrados en una transacción pueden ver que ocurre, al igual que cuando una persona entrega un billete de un dólar a un amigo. En el caso de un billete digital, el proceso de validación realizado por los participantes requiere que el destinatario pueda rastrear el billete hasta su origen, lo que a su vez implica ver a cada uno de los titulares anteriores del billete. En el contexto de Corda, esto se llama el "problema de la cadena trasera". Si bien el sistema no permite que todos vean todo, sí permite a los participantes tener una visión más allá de sus propias transacciones. Resolver el problema de la cadena trasera es un problema de diseño importante en los proyectos de CBDC del banco central. El desafío es organizar los asuntos para que realmente puedan emular los billetes de papel y preservar la privacidad transaccional de las personas.

Recientemente, los arquitectos de sistemas han estado explorando el uso de pruebas de conocimiento cero (ZKPs) para generar un registro criptográfico de que se ha producido una transacción, sin revelar ni la identidad de un participante ni el contenido de la transacción. Los ZKP permiten que una parte demuestre a otra que una declaración es verdadera sin revelar ninguna información más allá de ese hecho. En un sistema de pago, el objetivo es demostrar que el remitente de los fondos obtuvo esos fondos a través de una cadena legítima de transacciones, que se remonta e incluye la originación de los fondos, sin compartir ningún detalle de estas transacciones. El objetivo se logra reemplazando cada transacción individual con un ZKP y transfiriendo estas pruebas, en lugar de los detalles de la transacción individual, durante cada transacción sucesiva. Esta técnica permite a los destinatarios de un billete digital saber que se puede rastrear hasta su origen, sin conocer los detalles de la historia de este billete. En lugar de ver el historial de todas las transacciones anteriores, el verificador y, si lo desea, el notario, solo puede observar una serie de ZKPs (ver [Gráfico C1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxC-graC1)).

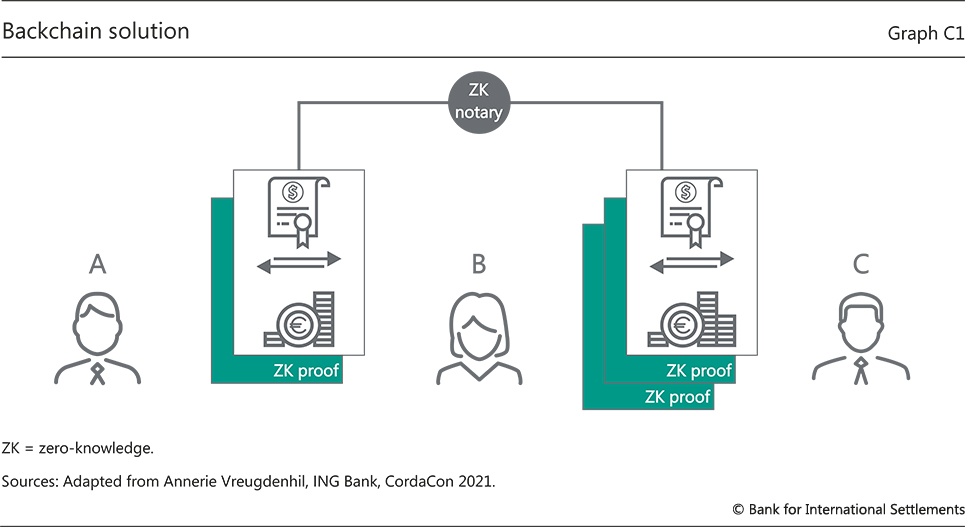
La técnica ZKP generalmente se entiende como un medio efectivo para generar privacidad transaccional, pero el uso de pruebas criptográficas erosiona el rendimiento del sistema al reducir su velocidad. Actualmente, los sistemas ZKP más populares son los llamados argumentos sucintos no interactivos de conocimiento (SNARKs), sucintos argumentos transparentes de conocimiento (STARKs) y Bulletproofs. Cada solución tiene diferentes costos en términos de verificación y tiempo de prueba general y tamaño de prueba general; estos se muestran en [la Tabla C1](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxC-tabC1). Los largos tiempos de verificación y prueba pueden reducir el rendimiento de las transacciones a niveles que son insuficientes para liquidar los volúmenes típicos del sistema de pago sin agregar una cantidad inaceptable de demora. Los investigadores están buscando formas de reducir estos tiempos.

**Cuadro C1**



Más allá de ZKP, la privacidad transaccional se puede lograr a través de otros medios, como el cifrado homomórfico, la computación segura de múltiples partes, la privacidad diferencial, las firmas ciegas, las firmas de anillo, los compromisos de Pedersen, la abstracción de cuentas y las direcciones ocultas. Cada una de estas metodologías emplea diferentes combinaciones de configuración confiable y / o sobrecarga computacional adicional. Actualmente, el BIS Innovation Hub está experimentando con direcciones ocultas, que son direcciones de un solo uso generadas por un protocolo, con el objetivo de ocultar las identidades de los participantes en una transacción.

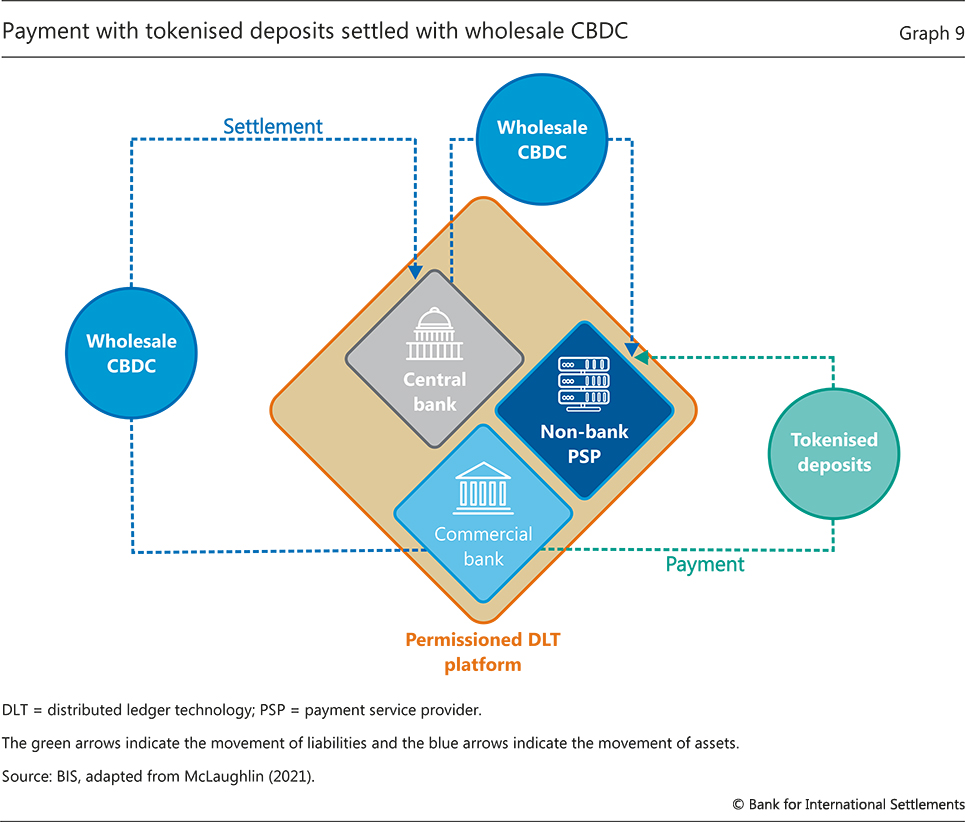
**Gráfico C1**



[icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#c1) Las transacciones no son totalmente anónimas en la medida en que, una vez que la información personal está vinculada a una dirección de billetera, todas las transacciones que usan esa dirección se pueden rastrear en la cadena de bloques.

Un posible sistema con depósitos tokenizados podría contar con una plataforma DLT autorizada. Esta plataforma registra todas las transacciones en tokens emitidos por las instituciones participantes, por ejemplo, bancos comerciales (que representan depósitos), PSP no bancarios (que representan dinero electrónico) y el banco central (que representa el dinero del banco central). Los inversores minoristas (depositantes) mantendrían tokens en billeteras digitales y realizarían pagos transfiriendo tokens a través de billeteras. La liquidación de transacciones entre instituciones financieras en la plataforma DLT se basaría en el uso de CBDC mayoristas como moneda de liquidación. Para tener una idea de cómo funcionaría esto, considere a un depositante que posee los tokens de un banco y desea realizar un pago al titular de tokens PSP no bancarios, que representan dinero electrónico, por ejemplo, para pagar una casa ([Gráfico 9](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra9)). Ambas partes pueden acordar que el pago (flecha verde) se produzca al mismo tiempo que se transfiere la escritura a la vivienda. En el fondo, para liquidar la transacción, el banco transferiría CBDC al por mayor en la plataforma DLT a la PSP no bancaria (flechas azules). El PSP no bancario transferiría una cantidad correspondiente de nuevos tokens a la billetera de su cliente. Todos estos pasos podrían ocurrir simultáneamente, como parte de una sola transacción atómica, ejecutada a través de contratos inteligentes. En este sistema, las CBDC al por mayor ayudan a liquidar transacciones y a garantizar la convertibilidad y uniformidad de las diversas representaciones del dinero. El mismo sistema también podría permitir representaciones digitales de acciones y bonos. Esto permitiría a los usuarios finales acceder fácilmente (fracciones de) estos activos en denominaciones pequeñas, las 24 horas del día, los 7 días de la semana, desde proveedores regulados, y liquidar las transacciones instantáneamente.

**Gráfico 9**



Las CBDC programables también podrían admitir pagos de máquina a máquina en ecosistemas autónomos.31 Las máquinas y dispositivos autónomos se comunican y ejecutan cada vez más procesos sin intervención humana a través del Internet de las Cosas, una red de dispositivos conectados. De cara al futuro, las máquinas pueden comprar directamente bienes y servicios entre sí, y administrar su propio presupuesto. Su interconexión aumentará la necesidad de contratos inteligentes y dinero programable. Por ejemplo, pueden estar equipados con billeteras, cargadas con un cierto presupuesto de dinero digital. Los contratos inteligentes pueden desencadenar automáticamente los pagos tan pronto como se cumplan ciertas condiciones, por ejemplo, la llegada de los bienes. Esto podría conducir a importantes ganancias de eficiencia, por ejemplo en el sector de la logística de mercancías, donde las transacciones a menudo tardan varios días y siguen siendo predominantemente en papel. Todo el potencial de estos desarrollos tecnológicos solo se puede realizar si las transacciones de máquina a máquina se liquidan instantáneamente, de modo que se elimine cualquier riesgo de liquidación. Los proyectos de criptomonedas del sector privado existentes para el Internet de las Cosas aún son exploratorios y sufren de límites a la escalabilidad.32 También plantean preocupaciones sobre la estabilidad y convertibilidad de las criptomonedas utilizadas para los pagos y requerirían puentes dentro y fuera de la rampa para conectarse con los rieles de pago tradicionales. En este sentido, la industria podría beneficiarse de las CBDC, que podrían apuntalar un sistema descentralizado, por ejemplo, permitiendo que las instituciones financieras reguladas emitan dinero programable.33

En resumen, la programabilidad, la componibilidad y la tokenización no son patrimonio de la criptografía. Los beneficios de la liquidación atómica y los protocolos de código abierto son totalmente compatibles con los bancos centrales que están en el centro del proceso de validación. Sin embargo, al depender del dinero del banco central, las CBDC al por mayor se beneficiarían de la estabilidad y la unicidad de la moneda que proporcionan los bancos centrales. También se basarían en la responsabilidad del banco central y de los intermediarios regulados ante la sociedad. Al apoyar los servicios innovadores del sector privado, facilitarían la adaptabilidad para que el sistema pueda satisfacer las nuevas necesidades a medida que surjan.

**CBDC minoristas y sistemas de pago rápido**

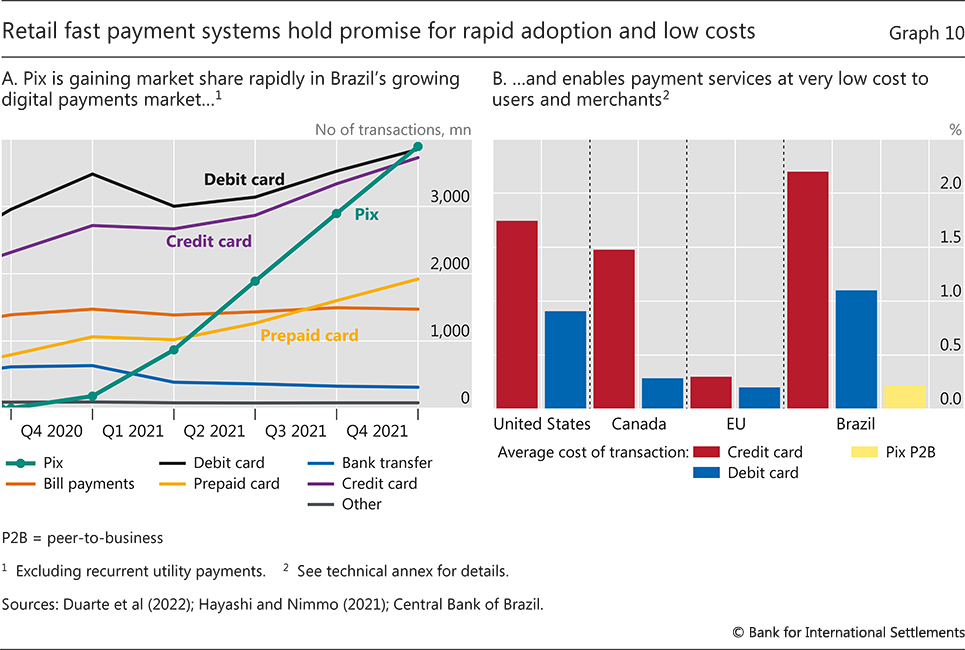
Las CBDC minoristas y los FPS minoristas comparten muchas similitudes. Las CBDC minoristas hacen que el dinero del banco central esté disponible en forma digital para hogares y empresas. Los PSP bancarios y no bancarios proporcionan servicios de pago minoristas. La diferencia clave con el FPS minorista es que, para las CBDC, el instrumento es un reclamo legal sobre el banco central. Por lo tanto, las CBDC minoristas a veces se ven como "efectivo digital", otra forma de dinero del banco central disponible para el público.34 En los FPS minoristas, muchos de los cuales son operados por el banco central, el instrumento que se intercambia es un reclamo a intermediarios privados (por ejemplo, depósitos bancarios o dinero electrónico). No obstante, tanto las CBDC minoristas como los FPS minoristas se basan en la arquitectura de datos públicos con API que garantizan el intercambio seguro de datos y la interoperabilidad entre diferentes PSP bancarios y no bancarios. Ambos cuentan con altas velocidades y disponibilidad, ya que las transferencias se producen en tiempo real o casi en tiempo real en una base (casi) 24/7.

Estas infraestructuras de pago minoristas ya han demostrado su valía para mejorar la eficiencia y la inclusión en el sistema monetario. A diferencia de la criptografía, que requiere altos alquileres y sufre de congestión y escalabilidad limitada, las CBDC y los FPS minoristas permiten que los efectos de red conduzcan a un círculo virtuoso de mayor uso, menores costos y mejores servicios. Debido a sus mandatos explícitos, los bancos centrales pueden diseñar sistemas para cumplir con estos objetivos desde cero. Un sistema de pago abierto que se base en la interoperabilidad de los servicios ofrecidos por los PSP privados competidores puede desafiar los alquileres en sectores bancarios concentrados y reducir los costos de pago para los usuarios finales.

Los FPS minoristas ya han logrado un progreso impresionante en la reducción de costos y el apoyo a la inclusión financiera para los no bancarizados. Por ejemplo, en poco más de un año después de su lanzamiento, el FPS minorista brasileño Pix es utilizado por dos tercios de la población adulta, con 50 millones de usuarios que realizan un pago digital por primera vez. Impulsados por productos y servicios innovadores ofrecidos por más de 770 PSP privados, los pagos Pix ahora han superado las transacciones con tarjetas de crédito y débito ([Gráfico 10.A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra10)). Los costos para los comerciantes de aceptar pagos de persona a empresa (P2B) promedian una décima parte del costo de los pagos con tarjeta de crédito ([Gráfico 10.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-gra10)). En otras economías se han logrado progresos igualmente impresionantes en los pagos inclusivos y de bajo costo.35

Las CBDC minoristas podrían desempeñar un papel igualmente beneficioso que los FPS minoristas, al tiempo que ofrecen capacidades tecnológicas adicionales. Por ejemplo, el Proyecto Hamilton, un proyecto conjunto del Banco de la Reserva Federal de Boston y la Iniciativa de Moneda Digital del Instituto de Tecnología de Massachusetts, ha demostrado la viabilidad técnica de una arquitectura CBDC que puede procesar 1,7 millones de transacciones por segundo, mucho más que las principales redes de tarjetas o blockchains.36 El proyecto utiliza funciones inspiradas en las criptomonedas, pero no utiliza DLT. En su próxima etapa, el Proyecto Hamilton tiene como objetivo crear una base para funcionalidades más complejas, como diseños criptográficos para la privacidad y la auditabilidad, la programabilidad y la autocustodia. El código para el proyecto es de código abierto y puede ser examinado por cualquier desarrollador, para maximizar el intercambio de conocimientos y ampliar el grupo de expertos que contribuyen a la base de código, incluidos los bancos centrales, el mundo académico y el sector privado.

**Gráfico 10**



Al igual que los FPS minoristas, las CBDC minoristas pueden diseñarse para apoyar la inclusión financiera.37 Muchos bancos centrales están explorando características de diseño de CBDC minoristas que abordan barreras específicas para la inclusión financiera, por ejemplo, a través de interfaces novedosas y pagos fuera de línea (véase [el recuadro D](https://www.bis.org/publ/arpdf/ar2022e3.htm#box-D)). Por ejemplo, el personal del Banco de Canadá ha investigado el potencial de los dispositivos de acceso universal dedicados que las personas podrían usar para almacenar y transferir de forma segura una CBDC. El Banco de Ghana ha explorado el uso de las redes existentes de agentes de dinero móvil y dispositivos portátiles.38 A través de billeteras CBDC escalonadas con diligencia debida simplificada para los usuarios que realizan transacciones en valores más pequeños, los bancos centrales pueden reducir el costo de los servicios de pago para los no bancarizados, fomentando así un mayor acceso a los pagos digitales y los servicios financieros. Al permitir que nuevas entidades (no bancarias) ofrezcan billeteras CBDC, también pueden superar la falta de confianza en las instituciones financieras que frena a muchas personas en el sistema actual.39

Tanto las CBDC minoristas como los FPS pueden diseñarse para proteger la privacidad y otorgar un mayor control del usuario sobre los datos. En la economía digital, cada transacción deja un rastro, lo que plantea preocupaciones sobre la privacidad, el abuso de datos y la seguridad personal. Además, los datos resultantes son de inmenso valor económico, que actualmente se acumula principalmente para las instituciones financieras y las grandes tecnológicas que recopilan, almacenan y monetizan los datos personales de los usuarios.

El poder sobre los datos de los PSP individuales se deriva del hecho de que, en los sistemas de pago convencionales, no existe un registro único y completo de todas las transacciones. En cambio, cada PSP mantiene un registro de sus propias transacciones solamente. Si bien los pagos a través de PSP se realizan a través de un sistema centralizado y requieren que las instrucciones se envíen a un operador central, estas instrucciones pueden implicar pagos por lotes o información incompleta sobre el propósito del pago. Por lo tanto, incluso el operador central no tiene una imagen completa de todos los pagos. Por lo tanto, la privacidad en los pagos se mantiene a través de una frágil combinación de mantenimiento de registros aislados y la promesa de confidencialidad por parte del operador central, pero no está garantizada. En algunos casos, las leyes de privacidad de datos brindan a los consumidores la oportunidad de otorgar o denegar el consentimiento de terceros para usar sus datos. Pero esta opción a menudo es difícil de ejercer de manera efectiva. Tal configuración implica que los consumidores no siempre saben si sus datos se están recopilando y con qué propósito.

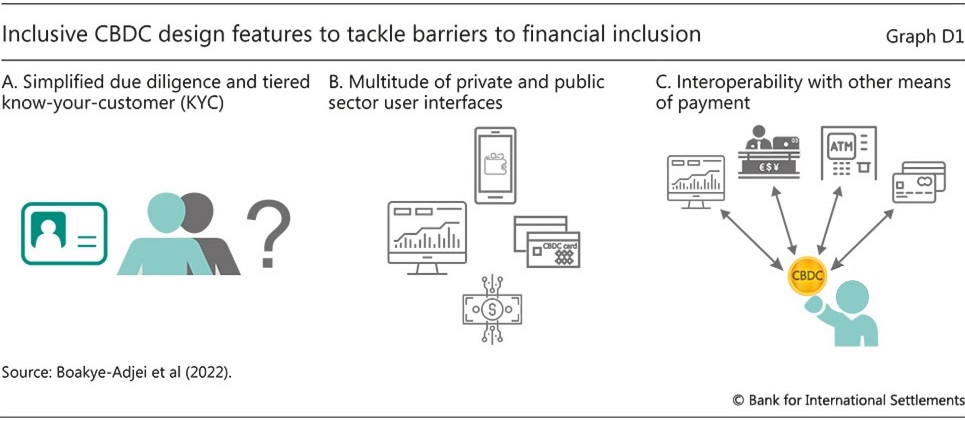
**Recuadro D**

**Diseñar CBDC minoristas para apoyar la inclusión financiera**

Muchos bancos centrales de todo el mundo ven la inclusión financiera como una motivación clave para su trabajo en cbdc minoristas. Esto es particularmente cierto en las economías de mercados emergentes y en desarrollo (EMDE), donde el acceso a los pagos digitales y otros servicios financieros está limitado por varias barreras clave. Estos incluyen (i) factores geográficos, por ejemplo, vastos territorios o islas; ii) factores institucionales y reglamentarios, como la falta de credenciales de identidad y la informalidad; iii) cuestiones económicas y de estructura de mercado, incluida la competencia limitada y los elevados costes en el sector financiero; iv) características de vulnerabilidad, por ejemplo, barreras por edad, sexo, ingresos o situación de discapacidad; v) la falta de oportunidades educativas y de educación financiera; y vi) la desconfianza en las instituciones financieras existentes. En muchos EMDE, la mayoría de los adultos carecen de acceso a opciones de pago digital.

Un nuevo estudio se basa en la experiencia de nueve bancos centrales de todo el mundo para abordar los desafíos de la inclusión financiera. [icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#f1) Concluye que algunos bancos centrales consideran que las CBDC son clave para su mandato como catalizador de la innovación y el desarrollo económico. Otros ven a las CBDC como un complemento potencial de las políticas existentes para apoyar la inclusión financiera. El estudio argumenta que, si se van a emitir CBDC, podrían diseñarse con varias características de diseño clave que aborden directamente las barreras a la inclusión financiera. Por ejemplo, podrían facilitar procesos de inscripción de clientes de bajo costo, por ejemplo, con diligencia debida simplificada, arreglos electrónicos de KYC y billeteras escalonadas, como se demuestra en varios sistemas de CBDC minoristas en vivo ([Gráfico D1. A](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxD-graD1)). Características como el uso de agentes externos ayudan a llegar a comunidades aisladas y a evitar la falta de confianza en las instituciones financieras. Los bancos centrales pueden ofrecer una infraestructura pública robusta y de bajo costo con una multitud de interfaces de usuario ([Gráfico D1.B](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxD-graD1)). Esto incluye la funcionalidad fuera de línea y las interfaces que se adaptan específicamente a los usuarios desatendidos. Y, por último, las CBDC fomentan la interoperabilidad tanto a nivel nacional como transfronterizo, contribuyendo así a una mayor competencia y a menores costes para los usuarios finales ([gráfico D1.C](https://www.bis.org/publ/arpdf/ar2022e3.htm#chap3-boxD-graD1)).

**Gráfico D1**



[icono](https://www.bis.org/publ/arpdf/ar2022e3.htm#e1) Boakye-Adjei et al (2022).

Los defensores de la criptografía argumentan que las cadenas de bloques sin permiso devuelven el control sobre los datos personales a los usuarios, pero un sistema basado en el pseudoanonimismo y un libro mayor público introduce graves riesgos para la privacidad y la integridad. También es incompatible con un sistema basado en nombres reales, que se requiere para garantizar la integridad y la rendición de cuentas.

La arquitectura de datos subyacente tanto a los FPS minoristas como a las CBDC puede dar un control mucho mayor al usuario sobre los datos personales, al tiempo que preserva la privacidad y el bienestar del consumidor. De hecho, los bancos centrales no tienen ningún interés comercial en los datos personales y, por lo tanto, pueden diseñar de manera creíble sistemas de interés público. Los sistemas de gobierno de datos pueden garantizar el consentimiento del usuario, la limitación del uso y las restricciones de retención.40 Al igual que la banca abierta, estas arquitecturas de datos también pueden permitir a los usuarios portar datos de manera que aporten beneficios económicos a los usuarios, por ejemplo, cuando solicitan un préstamo, desean utilizar servicios de planificación financiera o en una variedad de otros contextos. Es importante destacar que dicho sistema se basa en la identificación, y esta información de identidad a menudo puede ser retenida solo por el PSP y no por el banco central. El uso de la identificación también permite a los intermediarios financieros evaluar a los prestatarios para evaluar su solvencia, asegurando así que el escaso capital se asigne a su mejor uso.

En el proceso, los bancos centrales pueden hacer uso de la criptografía moderna, que ofrece soluciones para preservar la privacidad de los usuarios y garantizar la seguridad de las transacciones. Esto se puede lograr, por ejemplo, a través de ZKPs, que verifican la autenticidad de la transacción sin revelar su contenido ([recuadro C](https://www.bis.org/publ/arpdf/ar2022e3.htm#box-C)). No obstante, el sistema se basaría en las identidades verdaderas y verificadas de los usuarios, es decir, que realizarían transacciones bajo sus nombres reales. Varios bancos centrales también ven el "efectivo electrónico" en forma de CBDC minorista como una solución potencial para preservar la privacidad transaccional de las personas.41

Los diseños basados en la identidad son compatibles con la integridad en el sistema financiero. Con mandatos claros y responsabilidad pública, los sistemas pueden diseñarse para otorgar a las autoridades encargadas de hacer cumplir la ley acceso a la información con las salvaguardias legales requeridas. Estos enfoques ya son comunes en forma de leyes de secreto bancario y se están considerando para las CBDC minoristas.42 Es importante destacar que las transacciones no se registrarían en una cadena de bloques pública visible para todos. En el espacio corporativo, las nuevas soluciones de identidad digital corporativa podrían mejorar la supervisión de la propiedad real, reduciendo así el fraude, la elusión fiscal y la evasión de sanciones.43 Junto con las nuevas herramientas y capacidades de regtech inspiradas en el análisis de blockchain, existe el potencial para un mejor seguimiento de la actividad ilícita al tiempo que hace que el cumplimiento de los marcos regulatorios consuma menos recursos.

Finalmente, las CBDC minoristas y los FPS ofrecen oportunidades para mejorar la responsabilidad en relación con el sistema actual, y ciertamente en relación con el universo criptográfico. De hecho, el diseño de nuevas infraestructuras públicas no es una tarea exclusiva del banco central. Los nuevos sistemas requieren un diálogo público sobre el papel del banco central en los pagos minoristas. Su funcionamiento requerirá que se actualicen los mandatos legales, así como controles y equilibrios adecuados y formas apropiadas de rendición de cuentas del banco central a la sociedad. Es por esta razón que muchos bancos centrales han emitido consultas sobre estas iniciativas y están promoviendo el diálogo sobre la moneda de curso legal y las leyes de los bancos centrales.44 Un sistema basado en la infraestructura pública también garantizaría que los proveedores de servicios privados estén integrados en un marco normativo y de supervisión sólido. A diferencia de un sistema financiero criptográfico paralelo, las partes pueden rendir cuentas por sus acciones. En este nuevo ecosistema, es probable que haya nuevos modelos de negocio del sector privado que aún no se ajusten a los marcos regulatorios actuales, pero la experiencia hasta la fecha sugiere que los marcos pueden adaptarse para permitir nuevos tipos de actividad innovadora.45

**Lograr la integración transfronteriza**

Las cadenas de valor globales integradas significan que el mundo ya no es una colección de "economías insulares", sino más bien una densa red de interconexiones que requiere una matriz flexible de dinero, pagos y servicios financieros más amplios.46 Las CBDC mayoristas y minoristas, así como los FPS minoristas, pueden admitir la integración transfronteriza. Por lo tanto, el futuro sistema monetario será proporcional a la tarea de proporcionar vías sólidas de pago y liquidación que puedan apoyar la integración económica y los objetivos de interés público.

Los principios detrás de la construcción de plataformas multi-CBDC ilustran el potencial de la descentralización para ser aplicada de manera constructiva.47 En primer lugar, cuando hay más de una moneda involucrada, más de un banco central debe participar en la gobernanza de la plataforma de pago. Una forma de abordar el problema de la gobernanza entre múltiples partes es adoptar la descentralización a través de una plataforma DLT. Los notarios de confianza pueden administrar el libro mayor compartido, y los bancos centrales son los candidatos naturales para asumir esta tarea a nivel nacional, con infraestructura compartida a nivel mundial. En segundo lugar, dado que la descentralización debe lograrse utilizando nombres reales, en lugar de usar claves privadas como en las criptomonedas, salvaguardar la privacidad es un elemento de diseño esencial. El logro de ambos objetivos, el de respetar la privacidad mientras se usan nombres reales, se puede lograr mediante el uso de criptografía de clave pública.

Existen diferentes modelos para plataformas multi-CBDC, que van desde la simple coordinación de estándares, a través de sistemas de interconexión, hasta una plataforma mCBDC común y totalmente compartida. En una plataforma mCBDC común, las transferencias se registran en un solo libro mayor en un solo paso, y los participantes tienen visibilidad completa en tiempo real de sus saldos. El proceso de liquidación se simplifica así, obviando la necesidad de conciliación de saldos entre cuentas como en las transacciones bancarias corresponsales convencionales.

Una plataforma mCBDC común crea la oportunidad de simplificar los procesos. Por ejemplo, las reglas o condiciones de negocio se pueden automatizar utilizando las funciones de contrato inteligente en una plataforma DLT. Dicha automatización de procesos cosecha ganancias de eficiencia tanto en costos como en tiempo de transacción. Como los acuerdos mCBDC involucran a múltiples bancos centrales, cada uno con su propia moneda, la descentralización puede ser una característica constructiva, y la TRD autorizada puede desempeñar un papel importante. Además de las monedas de cada banco central en la plataforma, podría incluir tokens para otras monedas, incluidas las monedas internacionales. Estas plataformas tienen cierto parecido familiar con las utilizadas en criptografía y DeFi, como los contratos inteligentes y la programabilidad que permiten PvP o, en el contexto de los acuerdos de seguridad, DvP a través de las fronteras.

La vinculación de infraestructuras públicas a través de las fronteras también es posible para los FPS minoristas. Un proyecto reciente en el BIS Innovation Hub mostró el potencial de vincular FPS en diferentes jurisdicciones para que los pagos tomen segundos en lugar de días, reduciendo costos y haciendo que las tarifas y los tipos de cambio sean transparentes para los remitentes antes de que se comprometan a un pago. Lograr estos beneficios requiere coordinación en formatos de mensajería y en varias áreas políticas clave, pero es técnicamente factible.48

**Hacer un balance del progreso hacia la visión**

¿Cuál es la posición de los bancos centrales para lograr esta visión del futuro sistema monetario? Se están realizando esfuerzos sustanciales y los bancos centrales están trabajando juntos entre sí, con otras autoridades públicas y con el sector privado para ampliar la frontera de las capacidades en el sistema monetario.

A nivel mundial, un 90% de los bancos centrales encuestados recientemente están haciendo algún tipo de trabajo en CBDC mayoristas o minoristas.49 Se están llevando a cabo una serie de proyectos piloto mayoristas de CBDC, que a menudo involucran a varios bancos centrales en diferentes jurisdicciones. Hay tres CBDC minoristas en vivo y un total de 28 pilotos. Esto incluye el piloto a gran escala del Banco Popular de China, que ahora cuenta con 261 millones de usuarios.50 Mientras tanto, más de 60 jurisdicciones ahora tienen sistemas de pago rápido minorista, con varios más planeados en los próximos años, como FedNow en 2023.51 El BIS Innovation Hub está desarrollando plataformas mCBDC en asociación con los bancos centrales miembros. Estos son el Proyecto Jura (con los bancos centrales de Suiza y Francia), el Proyecto Dunbar (con Singapur, Malasia, Australia y Sudáfrica) y mBridge (con la RAE de Hong Kong, Tailandia, China y los Emiratos Árabes Unidos).

Un balance reciente del Centro de Innovación extrae lecciones de los experimentos de mCBDC hasta la fecha.52 Estos han demostrado su viabilidad desde una perspectiva técnica utilizando diferentes diseños experimentales. También han demostrado el potencial para una liquidación internacional mucho más rápida, de menor costo y más eficiente, sin la necesidad de intermediarios como los bancos corresponsales. En el lado minorista, el Innovation Hub, a través de sus centros de Hong Kong, Londres y los países nórdicos, está avanzando en el trabajo sobre arquitecturas ciberseguras, construyendo un ecosistema de API abierto para CBDC minoristas y explorando sistemas CBDC resistentes y fuera de línea.

Lograr pagos sin fricciones en el sistema monetario global requiere una fuerte cooperación entre los bancos centrales, combinada con la innovación en el sector privado. Apoyar estos esfuerzos es una ventaja comparativa del BPI que surge de su mandato para los asentamientos internacionales. De hecho, el BIS ya ha desarrollado pruebas de concepto y prototipos en entornos casi reales. Estos pueden ayudar a llamar la atención de los responsables de la formulación de políticas sobre los problemas reales que es probable que encuentren. También muestran que la cooperación es posible incluso cuando los bancos centrales adoptan diferentes enfoques para algunas cuestiones clave de política.

En resumen, los bancos centrales están trabajando juntos para promover los objetivos de política interna y apoyar un sistema monetario mundial perfectamente integrado con beneficios concretos para sus economías y usuarios finales. Las soluciones que utilizan se basarán en una gama de nuevas tecnologías, algunas inspiradas en el sistema monetario criptográfico, pero basadas en los sólidos marcos institucionales que existen hoy en día. Al adaptar el sistema ahora, los bancos centrales ayudarán a que el dinero y los pagos sean adecuados para las próximas décadas.

**Conclusión**

El sistema monetario es una base crucial para la economía. Cada vez que los hogares y las empresas realizan pagos en toda la gama de transacciones financieras, depositan su confianza en la seguridad del dinero y los sistemas de pago como un bien público. Mantener esta confianza es el núcleo de los mandatos de los bancos centrales.

Arraigado en esta confianza, el sistema monetario debe cumplir una serie de objetivos de alto nivel para servir a la sociedad. Debe ser seguro y estable, y las entidades clave deben rendir cuentas de sus acciones. De esta manera, se garantiza la integridad del sistema. Las transacciones rápidas, confiables y baratas deben promover la eficiencia y la inclusión financiera, mientras que los derechos de los usuarios a la privacidad y el control sobre los datos deben ser respetados. Finalmente, en un mundo en constante cambio y globalmente conectado, el sistema debe ser adaptable y abierto.

Los eventos recientes han demostrado cómo las fallas estructurales impiden que las criptomonedas alcancen los niveles de estabilidad, eficiencia o integridad requeridos para un sistema monetario. En lugar de servir a la sociedad, las criptomonedas y los DeFi están plagados de congestión, fragmentación y altos alquileres, además de las preocupaciones inmediatas sobre los riesgos de pérdidas e inestabilidad financiera.

Este capítulo ha presentado una visión más brillante del futuro sistema monetario. Alrededor del núcleo de la confianza proporcionada por el dinero del banco central, el sector privado puede adoptar lo mejor que las nuevas tecnologías tienen para ofrecer, incluida la programabilidad, la componibilidad y la tokenización, para fomentar un ecosistema monetario vibrante. Esto se logrará a través de rieles de pago avanzados como CBDC y FPS minoristas.

Una asociación público-privada en estas líneas podría hacer que el sistema monetario sea más adaptable y abierto a través de las fronteras. Dentro de una década, los usuarios pueden dar por sentados los pagos en tiempo real y de bajo costo, y los pagos a través de las fronteras pueden ser tan fluidos como el intercambio transfronterizo que apoyan. Debe aumentarse la elección de los consumidores en los servicios financieros, y la innovación continuará empujando las fronteras de lo que es posible.

En todo esto, la innovación debe partir de la comprensión de las necesidades concretas de los hogares y las empresas en la economía real, y de las demandas políticas que imponen a un sistema monetario. Si bien las tecnologías descentralizadas como DLT ofrecen muchas posibilidades, las necesidades de los usuarios deben mantenerse a la vanguardia de la innovación privada, al igual que el interés público sigue siendo el lodestar para los bancos centrales.

Tanto en el diseño de nuevas infraestructuras como en la regulación, existe una necesidad continua de cooperación global entre los bancos centrales y, de hecho, una amplia gama de nuevas partes interesadas. Apoyar esta cooperación seguirá siendo un objetivo clave del BPI.

**Notas**

[1](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_1) Consulte las [Estadísticas del Libro Rojo del BIS](https://stats.bis.org/statx/toc/CPMI.html), que recopilan datos sobre pagos minoristas sin efectivo en 27 países.

[2](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_2) Véase Giannini (2011); Borio (2018)); Carstens (2019).

[3](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_3) Véase BIS CPMI (2016); BIS (2021).

[4](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_4) En la actualidad, no existen directrices claras y armonizadas sobre quién puede servir como oráculo, o quién es responsable si un contrato inteligente actúa sobre información incorrecta fuera de la cadena. Como es imposible escribir ex ante un contrato inteligente que cubra todas las contingencias posibles, se necesita cierto grado de centralización para resolver disputas.

[5](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_5) La seguridad en DLT se refiere a la solidez del consenso, es decir, la confianza en que el libro mayor compartido es preciso. La seguridad puede verse amenazada por actores maliciosos que comprometen el libro mayor para ejecutar transacciones fraudulentas, como en un ataque del 51% (ver glosario).

[6](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_6) Véase el glosario para una definición, Schär (2021) para una descripción en profundidad, y Aramonte et al (2021) y Carter y Jeng (2021) para una evaluación de los riesgos y la descentralización. Cabe destacar que, incluso si DeFi a menudo se basa en DLT anónimo y sin permiso para lograr la descentralización, DLT autorizado también permite el uso de contratos inteligentes y la componibilidad asociada (Auer (2022)). En este caso, un conjunto de validadores centralizados se encargan de validar las transacciones.

[7](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_7) Véase Aramonte et al (2021).

[8](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_8) Véase Arner et al (2019); Catalini y de Gortari (2021); Frost et al (2021); Gorton y Zhang (2021).

[9](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_9) Véase Brainard (2021); Garratt et al (2022).

[10](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_10) Véase Allen (2022).

[11](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_11) Véase BIS (2018), Auer (2019); Auer et al (2021).

[12](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_12) El límite es de alrededor de cuatro transacciones por segundo para Bitcoin y 30 para Ethereum. Las posibles soluciones al problema de las rentas elevadas derivadas de la escalabilidad de la congestión (por ejemplo, a través de "sharding") suelen introducir una mayor complejidad tecnológica y requieren un mayor grado de centralización en la estructura de gobierno. Además, la sostenibilidad de la estructura de incentivos aún no se comprende completamente.

[13](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_13) Los puentes se pueden dividir en dos tipos principales: "centralizados" y "sin confianza". Las diferencias radican en cómo se confirman las transacciones puente y cómo se almacenan los activos depositados. En un sistema centralizado, una red de validadores preseleccionados rastrea los depósitos de tokens en la cadena de origen, los bloquea y acuña tokens en la cadena de destino. En un sistema sin confianza, cualquiera puede convertirse en un validador. Para cada transacción puente, los validadores se seleccionan aleatoriamente de un grupo para minimizar los riesgos de manipulación. En ambos casos, las actividades de consenso y custodia son realizadas por un número limitado de validadores.

[14](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_14) La necesidad de garantías en muchas transacciones también es perjudicial para lograr un sistema inclusivo. Requerir una garantía significa que se necesita dinero para pedir dinero prestado. Por ejemplo, a menos que los usuarios ya tengan fondos suficientes en forma de criptomoneda para publicar como garantía, no pueden pedir prestada otra criptomoneda en las plataformas de préstamos. Véase Aramonte et al (2022).

[15](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_15) Véase IOSCO (2022).

[16](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_16) Como se discutió anteriormente, estas "tarifas de gas" están diseñadas para compensar a los validadores. Aunque los costos de transacción son más altos en los DEX, algunos operadores prefieren estas plataformas, en parte debido a su mayor anonimato e interoperabilidad con otras aplicaciones DeFi.

[17](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_17) Véase SEC (2022).

[18](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_18) Véase CPMI-IOSCO (2021); Carstens et al (2021).

[19](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_19) Véase Auer, Frost y Vidal Pastor (2022).

[20](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_20) Véase Brummer (2022).

[21](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_21) Véase BCBS (2021); Auer et al (2022).

[22](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_22) Tether, la moneda estable más grande por capitalización de mercado, según los informes, mantiene la mitad de sus reservas en certificados de depósito y papel comercial (actualmente alrededor de USD 25 mil millones en total), lo que la convierte en un importante inversor en este mercado.

[23](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_23) BCBS (2021).

[24](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_24) Véase Carstens (2022); BIS (2021); BIS (2020); CPSS (2003).

[25](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_25) Véase Garratt et al (2022); McLaughlin (2021) aboga más ampliamente por una red de "pasivos regulados tokenizados" y de activos.

[26](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_26) Véase Schnabel y Shin (2004, 2018).

[27](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_27) Véase Boar et al (2021).

[28](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_28) Véase BIS (2021).

[29](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_29) Véase Bech et al (2020).

[30](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_30) Véase Garratt et al (2022); McLaughlin (2021).

[31](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_31) Véase Deutsche Bundesbank (2020); Forster et al (2020); Pocher y Zichichi (2022).

[32](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_32) Véase Mercan et al (2021).

[33](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_33) Ver Forster et al (2020) y Bechtel et al (2022) para una discusión de estas características.

[34](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_34) En una CBDC, un pago solo implica transferir un reclamo directo al banco central de un usuario final a otro. Los fondos no pasan por encima del balance de un intermediario, y las transacciones se liquidan directamente en dinero del banco central, en el balance del banco central y en tiempo real. Por el contrario, en un FPS, el beneficiario minorista recibe fondos finales de inmediato, pero la liquidación mayorista subyacente entre PSP puede aplazarse (véase Carstens (2021)).

[35](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_35) Véase BIS CPMI (2021). La interfaz de pago unificada en la India y Bakong en Camboya han visto una adopción y promoción particularmente rápidas de los objetivos de inclusión financiera.

[36](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_36) Véase Lovejoy et al (2022). En comparación, las principales redes de tarjetas pueden procesar varios miles de transacciones por segundo, y Ethereum procesa 30 por segundo.

[37](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_37) Véase Carstens y Su Majestad la Reina Máxima (2022).

[38](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_38) Véase Miedema et al (2020); Banco de Ghana (2022).

[39](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_39) Véase Gjefle et al (2021). En los Estados Unidos, la desconfianza en los bancos y la incertidumbre en torno a las transacciones son desafíos persistentes para las personas no bancarizadas.

[40](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_40) Véase Tiwari et al (2022).

[41](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_41) Véase CGIDE (2020); BCE (2020).

[42](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_42) Por ejemplo, en las Bahamas, el banco central no tiene acceso a la información de identidad individual de los usuarios de CBDC y solo compartirá información de transacciones con la policía si se emite una orden judicial. Véase Boakye-Adjei et al (2022).

[43](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_43) Véase Leung et al (2022).

[44](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_44) Véase, por ejemplo, Junta de Gobernadores del Sistema de la Reserva Federal (2022); BCE (2020); Banco de Inglaterra (2022); Banco de Japón (2020); Sveriges Riksbank (2021).

[45](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_45) Por ejemplo, algunas jurisdicciones han definido nuevas funciones para los intermediarios privados en el sistema monetario, como los proveedores de servicios de iniciación de pagos (UE), los proveedores de aplicaciones de terceros (India) o los bancos virtuales (China, la RAE de Hong Kong, Corea). Esto a menudo da lugar a nuevos requisitos reglamentarios adaptados a las actividades recién definidas.

[46](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_46) Por ejemplo, la producción de bienes intermedios en múltiples economías requiere un volumen creciente de crédito. Véase BIS (2017); Shin (2017).

[47](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_47) Véase Auer et al (2021) y glosario.

[48](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_48) Véase BIS Innovation Hub (2021).

[49](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_49) Véase Kosse y Mattei (2022).

[50](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_50) Véase Auer et al (2020), actualizado hasta enero de 2022.

[51](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_51) Véase BIS CPMI (2021).

[52](https://www.bis.org/publ/arpdf/ar2022e3.htm#fn_52) Véase BIS Innovation Hub (2022); BISIH et al (2021, 2022).

**Anexo técnico**

Gráfico 1: Valores de fin de semana. Las categorías comprenden las nueve monedas estables más grandes, 59 monedas DeFi y otras 56 criptomonedas. Las monedas DeFi corresponden a criptomonedas emitidas por plataformas DeFi y con una capitalización de mercado a valor total bloqueado ratio inferior a 50, según informa DeFi Llama. El valor total bloqueado se refiere al tamaño de los grupos de capital que sustentan los protocolos DeFi. Para obtener más información, consulte la Tabla A2 de Auer (2022).

Gráfico 2.A: Valores atípicos mayores de 450 Gwei (10–9 ETH) se excluyen del gráfico.

Gráfico 4.A: Basado en puentes y protocolos cross-chain.

Gráfico 5.A: Los costos de transacción se miden como el diferencial relativo de oferta y demanda, definido como 2 \* (precio de venta - precio de oferta) / (precio de venta + precio de oferta) para Tether-Ether. Centralizado es un promedio simple de los intercambios criptográficos Coinbase y Binance. Decentralised se basa en Uniswap. Promedios semanales de valores diarios.

Gráfico 5.B: Centralizado = Binance, Coinbase y FTX; Descentralizado = Curve.fi, PancakeSwap (v2) y Uniswap (V2).

Gráfico 6.B: Empresas con un enfoque en tecnologías de criptomonedas. La lista completa de las empresas está disponible en www.blockdata.tech/blog/general/banks-investing-blockchain-companies.

Gráfico 10.B: Para los Estados Unidos, Canadá y la UE, promedio de las tasas de intercambio en las tarjetas de crédito y débito. El costo total para los comerciantes puede ser mayor.

Gráfico A1. B: El precio corresponde al precio bajo.

Gráfico B1. R: Promedios mensuales entre países de usuarios activos diarios.

Gráfico B1. C: Disposición a asumir riesgos financieros para los consumidores estadounidenses de 20 a 79 años. Promedio ponderado (por ponderaciones de la encuesta) entre los encuestados. La muestra cubre el período de enero de 2020 a julio de 2021.

**Referencias**

Allen, H (2022), "We're asking the wrong questions about stablecoins", *Financial Times*, 2 de junio.

Aramonte, S, W Huang y A Schrimpf (2021): "[DeFi risks and the decentralisation illusion](https://www.bis.org/publ/qtrpdf/r_qt2112b.htm)", *BIS Quarterly Review*, diciembre.

Aramonte, S, S Doerr, W Huang y A Schrimpf (2022): "[DeFi lending: intermediation without information?](https://www.bis.org/publ/bisbull57.htm)", *BIS Bulletin*, no 57, junio.

Arner, D, R Auer y J Frost (2020): "[Stablecoins: risks, potential and regulation](https://www.bis.org/publ/work905.htm)", *Bank of Spain Financial Stability Review*, noviembre.

Auer, R (2019): "[Beyond the doomsday economics of "proof-of-work](https://www.bis.org/publ/work765.htm)" in cryptocurrencies", *BIS Working Papers*, no 765, enero.

--- (2022): "Supervisión integrada: cómo incorporar la regulación en las finanzas descentralizadas", *Cryptoeconomic Systems*, de próxima aparición.

Auer, R, P Haene y H Holden (2021): "[Multi-CBDC arrangements and the future of cross-border payments](https://www.bis.org/publ/bppdf/bispap115.htm)", *BIS Papers*, n.º 115, marzo.

Auer, R, G Cornelli y J Frost (2020): "[Rise of the central bank digital currencies: drivers, approaches and technologies](https://www.bis.org/publ/work880.htm)", *BIS Working Papers*, no 880, agosto.

Auer, R, G Cornelli, S Doerr, J Frost y L Gambacorta (2022): "¿Encadenados a la especulación? Feedback trading in crypto markets", *BIS Working Papers, de* próxima aparición.

Auer, R, M Farag, U Lewrick, L Orazem y M Zoss (2022): "¿[Banca a la sombra de Bitcoin?](https://www.bis.org/publ/work1013.htm) La adopción institucional de las criptomonedas", *BIS Working Papers*, no 1013, mayo.

Auer, R, J Frost y J Vidal Pastor (2022): "[Los mineros como intermediarios: valor extraíble y manipulación del mercado en cripto y DeFi](https://www.bis.org/publ/bisbull58.htm)", *Bis Bulletin*, no 58, junio.

Auer, R, C Monnet y H S Shin (2021): "[Distributed ledgers and the governance of money](https://www.bis.org/publ/work924.htm)", *BIS Working Papers*, no 924, enero.

Auer, R y D Tercero-Lucas (2021): "¿[Desconfianza o especulación? Los impulsores socioeconómicos de las inversiones en criptomonedas de los Estados Unidos](https://www.bis.org/publ/work951.htm)", *BIS Working Papers*, no 951, julio.

Banco de Inglaterra (2022): *Respuestas al documento de debate del Banco de Inglaterra sobre nuevas formas de dinero digital*, marzo.

Banco de Ghana (2022): *Documento de diseño del Cedi digital (eCedi),* marzo.

Banco de Japón (2020): *El enfoque del Banco de Japón a la moneda digital del banco central*, octubre.

Comité de Supervisión Bancaria de Basilea (BCBS) (2021): [*Tratamiento prudencial de las exposiciones a criptoactivos*](https://www.bis.org/bcbs/publ/d519.htm), documento consultivo, junio.

Bech, M, C Boar, D Eidan, P Haene, H Holden y W Toh (2022): "[Using CBDCs across borders: lessons from practical experiments](https://www.bis.org/publ/othp51.htm)", BIS Innovation Hub, junio.

Bech, M, J Hancock, T Rice y A Wadsworth (2020): "[Sobre el futuro de la liquidación de valores](https://www.bis.org/publ/qtrpdf/r_qt2003i.htm)" *BIS Quarterly Review*, marzo.

Bechtel, A, A Ferreira, J Gross y P Sandner (2022): *El futuro de los pagos en una economía europea basada en DLT: una hoja de ruta*, Instituto Alemán de Estudios Japoneses.

Banco de Pagos Internacionales (BPI) (2017): "[Understanding globalisation](https://www.bis.org/publ/arpdf/ar2017e6.htm)", *87º Informe Anual,* junio, Capítulo IV,

--- (2018): "[Cryptocurrencies: looking beyond the hype](https://www.bis.org/publ/arpdf/ar2018e5.htm)", *Informe Económico Anual 2018*, junio, Capítulo V.

--- (2020): "[Bancos centrales y pagos en la era digital](https://www.bis.org/publ/arpdf/ar2020e3.htm)", *Informe Económico Anual 2020*, junio, capítulo III.

--- (2021): "[CBDCs: an opportunity for the monetary system](https://www.bis.org/publ/arpdf/ar2021e3.htm)", *Informe Económico Anual* 2021, junio, capítulo III.

Bis Committee on Payments and Market Infrastructures (BIS CPMI) (2016): [*Pagos rápidos: mejora de la velocidad y la disponibilidad de los pagos minoristas*](https://www.bis.org/cpmi/publ/d154.htm), noviembre.

--- (2021): [*Evolución de los pagos rápidos al por menor e implicaciones para los sistemas SLBTR*](https://www.bis.org/cpmi/publ/d201.htm), diciembre.

BIS Innovation Hub (BISIH) (2021): "[Nexus: a blueprint for instant cross-border payments](https://www.bis.org/publ/othp39.htm)", julio.

--- (2022): "Profundiza en la experiencia adquirida a través de los proyectos multi-CBDC de BIS Innovation Hub", mimeo.

BISIH, Banco de la Reserva de Australia (RBA), Banco Nacional de Malasia (NBM), Autoridad Monetaria de Singapur (MAS) y Banco de la Reserva de Sudáfrica (SARB) (2022): "[Proyecto Dunbar – Asentamientos internacionales utilizando multi-CBDC](https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm)", marzo.

BISIH, Hong Kong Monetary Authority (HKMA), Bank of Thailand (BoT), Digital Currency Institute of the People's Bank of China (PBC) y Central Bank of the United Arab Emirates (CBUAE) (2021): "[Inthanon-LionRock to mBridge: Building a multi-CBDC platform for international payments](https://www.bis.org/publ/othp40.htm)", septiembre.

Boakye-Adjei, N, R Auer, J Frost, J Prenio, H Banka, A Faragallah y H Natarajan (2022): "[Central bank digital currencies (CBDCs): a new tool in the financial inclusion toolkit?"](https://www.bis.org/fsi/publ/insights41.htm), *FSI Insights*, abril.

Boar, C, S Claessens, A Kosse, R Leckow y T Rice (2021): "[Interoperability between payment systems across borders](https://www.bis.org/publ/bisbull49.htm)", *Bis Bulletin*, n.º 49, diciembre.

Junta de Gobernadores del Sistema de la Reserva Federal (2022): "Dinero y pagos: el dólar estadounidense en la era de la transformación digital", enero.

Boissay, F, G Cornelli, S Doerr y J Frost (2022): "[Escalabilidad de Blockchain y la fragmentación de la criptografía](https://www.bis.org/publ/bisbull56.htm)", *BIS Bulletin*, no 56, junio.

Borio, C (2019): "[On money, debt, trust and central banking](https://www.bis.org/speeches/sp181115.pdf)", *BIS Working Papers*, no 763, enero.

Brainard, L (2021): "Private money and central bank money as payments go digital: an update on CBDCs", discurso en la Conferencia Consensus by CoinDesk 2021, Washington DC, 24 de mayo.

Brummer, C (2022): "Disclosure, Dapps and DeFi", *Stanford Journal of Blockchain Law and Policy*, de próxima aparición.

Buterin, V (2021): "Por qué la fragmentación es genial: desmitificando las propiedades técnicas", vitalik.ca/general/2021/04/07/sharding.htm.

Carstens, A, S Claessens, F Restoy y H S Shin (2021): "[Regulating big techs in finance](https://www.bis.org/publ/bisbull45.htm)", *BIS Bulletin*, no 45, agosto.

Carstens, A (2022): "[Las monedas digitales y el alma del dinero](https://www.bis.org/speeches/sp220118.htm)", discurso en la Universidad Goethe, 18 de enero.

--- (2021): "[Las monedas digitales y el futuro del sistema monetario](https://www.bis.org/speeches/sp210127.htm)", comentarios en el seminario de política de la Institución Hoover, 27 de enero.

--- (2019): "[El futuro del dinero y el sistema de pago: ¿qué papel desempeñan los bancos centrales?"](https://www.bis.org/speeches/sp191205.htm), conferencia en la Universidad de Princeton, 5 de diciembre.

Carstens, A y Su Majestad la Reina Máxima (2022): "[CBDCs for the people](https://www.bis.org/speeches/sp220418.htm)", *Project Syndicate*, 18 de abril.

Carter, N y L Jeng (2021): "DeFi protocol risks: the paradox of DeFi", en B Coen y D Maurice (eds), *Regtech, suptech and beyond: innovation and technology in financial services*, RiskBooks.

Catalini, C y A de Gortari (2021): *"*Sobre el diseño económico de stablecoins", mimeo.

Comité de Pagos y Sistemas de Liquidación (2003): [*The role of central bank money in payment systems*](https://www.bis.org/cpmi/publ/d55.htm), 12 de agosto.

CPMI y Organización Internacional de Comisiones de Valores (IOSCO) (2021): [*Aplicación de los Principios para las Infraestructuras de los Mercados Financieros a los acuerdos de stablecoin*](https://www.bis.org/cpmi/publ/d198.htm), octubre.

Comparitech (2022), [Worldwide cryptocurrency heists tracker](https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/), febrero.

Grupo Consultivo para la Innovación y la Economía Digital (CGIDE) (2020): [*Habilitación de la financiación abierta a través de APIs*](https://www.bis.org/publ/othp36.htm), diciembre.

Deutsche Bundesbank (2020): *Money in programmable applications*, informe del Grupo de Trabajo sobre Dinero Programable, diciembre.

Duarte, A, J Frost, L Gambacorta, P Koo Wilkens y H S Shin (2022): "[Bancos centrales, el sistema monetario y las infraestructuras públicas de pago: lecciones del Pix de Brasil](https://www.bis.org/publ/bisbull52.htm)", *Boletín BIS*, no 52, marzo.

Banco Central Europeo (BCE) (2020): *Informe sobre un euro digital*, octubre.

Foley, S, J Karlsen y T Putnins (2019): "Sexo, drogas y Bitcoin: ¿cuánta actividad ilegal se financia a través de criptomonedas?", *Review of Financial Studies*, vol 32, no 5, pp 1798-853.

Forster, M, J Gross, A Kamping, S Katilmis, M Reichel, P Sandner y P Schröder (2020): "El futuro de los pagos: pagos programables en el sector IoT", mimeo.

Frost, J, P Wierts y H S Shin (2020): "¿[Una stablecoin temprana? El Banco de Ámsterdam y la gobernanza del dinero](https://www.bis.org/publ/work902.htm)", *BIS Working Papers*, nº 902, noviembre.

Garratt, R, M Lee, A Martin y J Torregrossa (2022): "El futuro de los pagos no son stablecoins", *Liberty Street Economics*, 7 de febrero.

Giannini, C (2011): *La era de los bancos centrales*, Edward Elgar.

Gjefle, E, Z Herring, C Kubli, B O'Rea y G Rakusen, G (2021): *Centrando a los usuarios en el diseño de moneda digital*, MIT Digital Currency Institute y Maiden Labs.

Gorton, G y J Zhang (2022): "Taming wildcat stablecoins", *University of Chicago Law Review*, vol 90, de próxima aparición.

Hayashi, F y V Nimmo (2021): "Tarifas de intercambio de tarjetas de crédito y débito en varios países. Actualización de agosto de 2021", Banco de la Reserva Federal de Kansas City, Payments System Research.

Hileman, G (2015): "The Bitcoin market potential index", Proceedings of the Second Workshop on Bitcoin Research in Association with Financial Cryptography and Data Security, Springer.

Organización Internacional de Comisiones de Valores (IOSCO) (2022): *Informe financiero descentralizado de la IOSCO*, marzo.

Kosse, A e I Mattei (2022): "[Ganando impulso – Resultados de la encuesta BIS 2021 sobre monedas digitales del banco central](https://www.bis.org/publ/bppdf/bispap125.htm)", *BIS Papers*, no 125, mayo.

Knittel, M, S Pitts y R Wash (2019): "'The most trustworthy coin: how ideological tensions drive trust in Bitcoin", *Proceedings of the ACM on Human-Computer Interaction*, vol 3, no 36, pp 1-23.

Leung, D, D Arner, J Frost y B Nolens (2022): "[Identidad digital corporativa: ¿no hay bala de plata, sino un lado positivo?"](https://www.bis.org/publ/bppdf/bispap126.htm), *BIS Papers*, junio.

Lovejoy, J, C Fields, M Virza, T Frederick, D Urness, K Karwaski, A Brownworth y N Narula (2022): "Un sistema de procesamiento de pagos de alto rendimiento diseñado para monedas digitales del banco central", febrero.

McLaughlin, T (2021): "The regulated internet of value", Citi Treasury and Trade Solutions.

Mercan, S, A Kurt, E Erdin y K Akkaya (2021): "Soluciones de criptomonedas para permitir micropagos en IoT de consumo", Universidad de Cornell, febrero.

Miedema, J, C Minwalla, M Warren y D Shah (2020): "Designing a CBDC for universal access", *Bank of Canada Staff Analytical Notes*, no 2020-10.

Pocher, N y M Zichichi (2022): "Hacia los pagos de máquina a máquina basados en CBDC en ioT de consumo", 37ésimo Simposio ACM/SIGAPP sobre Computación Aplicada, abril.

Schär, F (2021): "Finanzas descentralizadas: en los mercados financieros basados en blockchain y contratos inteligentes", *Federal Reserve Bank of St. Louis Review*, vol 103, no 2, abril.

Schnabel, I y H S Shin (2004): "Liquidez y contagio: la crisis de 1763", *Journal of the European Economic Association*, vol 2, no 6, pp 929-68, diciembre.

--- (2018): "[Money and trust: lessons from the 1620s for money in the digital age](https://www.bis.org/publ/work698.htm)", *BIS Working Papers*, no 698, febrero.

Comisión de Bolsa y Valores (SEC) (2022): *Boletín de Contabilidad del Personal*, n.º 121, marzo.

Shin, H S (2017): "[Globalización: real y financiera](https://www.bis.org/speeches/sp170625b.htm)", discurso en la Asamblea General Anual del BIS, 25 de junio.

Sveriges Riksbank (2022): "E-krona pilot Phase 2", abril.

Swartz, L (2020): *New money: how payment became social media*, Yale University Press.

Tiwari, S, S Sharma, S Shetty y F Packer (2022): "[The design of a data governance system](https://www.bis.org/publ/bppdf/bispap124.htm)", *BIS Papers*, no 124, mayo.

**Glosario**

Ataque del 51%: Cuando un actor malicioso es capaz de comprometer a más de la mitad de los validadores en la red, el actor puede ejecutar transacciones fraudulentas.

Interfaz de programación de aplicaciones (API): un conjunto de reglas y especificaciones seguidas por programas de software para comunicarse entre sí, y una interfaz entre diferentes programas de software que facilita su interacción.

Liquidación atómica: intercambio instantáneo de dos activos, de modo que la transferencia de uno ocurre solo después de la transferencia del otro.

Blockchain: una forma de libro mayor distribuido sin permiso en el que los detalles de las transacciones se mantienen en el libro mayor en forma de bloques de información.

Bienes públicos del banco central: bienes y servicios proporcionados por el banco central que sirven al interés público, incluidas las infraestructuras de pago y la confianza en la moneda.

Componibilidad: la capacidad de combinar diferentes componentes en un sistema, como los protocolos DeFi.

Consenso: en las aplicaciones DLT, el proceso por el cual los validadores acuerdan el estado de un libro mayor distribuido.

Criptomoneda (también criptoactivo o criptografía): un tipo de activo digital del sector privado que depende principalmente de la criptografía y el libro mayor distribuido o tecnología similar.

Arquitectura de datos: como se utiliza aquí, la combinación de interfaces de identificación y programación de aplicaciones que permite el uso seguro de los datos.

Aplicaciones descentralizadas (dApps): Aplicaciones DeFi que ofrecen servicios como préstamos o comercio, predominantemente entre criptomonedas y stablecoins.

Intercambios descentralizados (DEX): mercados donde las transacciones ocurren directamente entre comerciantes de criptomonedas o stablecoins.

Finanzas descentralizadas (DeFi): un conjunto de actividades en todos los servicios financieros basadas en DLT sin permiso, como las cadenas de bloques.

Billetera digital: una interfaz que permite a los usuarios realizar transferencias o realizar transacciones de otra manera en dinero y activos digitales.

Tecnología de contabilidad distribuida (DLT): un medio para guardar información a través de un libro mayor distribuido, es decir, una copia digital repetida de los datos disponibles en múltiples ubicaciones.

Tarifas de gas: unidad que mide la cantidad de esfuerzo computacional requerido para ejecutar operaciones específicas en la red Ethereum. Gas se refiere a la tarifa requerida para realizar una transacción en Ethereum con éxito.

Internet de las cosas: software, sensores y conectividad de red integrados en dispositivos físicos, edificios y otros elementos que permiten a esos objetos (i) recopilar e intercambiar datos y (ii) enviar, recibir y ejecutar comandos, incluidos los pagos.

Nivel 1: las cadenas de bloques competidoras a veces se denominan redes de "nivel 1", para distinguirlas de las redes separadas fuera de la cadena ("nivel 2") que registran transacciones fuera del libro mayor distribuido.

Integridad del mercado: la prevención de actividades ilícitas en el sistema monetario, como el lavado de dinero y el financiamiento del terrorismo, así como la manipulación del mercado.

Sistema monetario: el conjunto de instituciones y arreglos en torno al intercambio monetario. Esto consta de dos componentes: dinero y sistemas de pago.

Acuerdos multi-CBDC: soluciones para hacer compatibles las CBDC, interconectar los sistemas CBDC o crear un sistema compartido para pagos transfronterizos y transdivisa CBDC.

Tokens no fungibles (NFT): tokens criptográficos únicos que existen en una cadena de bloques y no se pueden replicar, utilizados para representar la propiedad de, por ejemplo, obras de arte, bienes raíces u otros activos.

Banca abierta: el intercambio y aprovechamiento de datos autorizados por el cliente por parte de los bancos con desarrolladores y empresas de terceros para crear aplicaciones y servicios.

Código abierto: una característica mediante la cual el código fuente original se pone a disposición del público.

Oracle: un servicio que proporciona información externa ("fuera de la cadena") para su uso por contratos inteligentes en un sistema DLT.

DLT autorizado: una forma de DLT mediante la cual solo un grupo predefinido de instituciones de confianza puede actuar como un nodo de validación.

DLT sin permiso: una forma de DLT donde cualquier participante puede actuar como un nodo de validación, por ejemplo, con cadenas de bloques (sin permiso).

Programabilidad: una característica de DLT y otras tecnologías mediante la cual las acciones pueden programarse o automatizarse.

Prueba de participación: un método por el cual los validadores prometen o "apuestan" monedas que se utilizan como incentivo para que las transacciones agregadas al libro mayor distribuido sean válidas.

Prueba de trabajo: un método por el cual los validadores compiten para realizar cálculos matemáticos para verificar y agregar transacciones al libro mayor distribuido.

Pseudoanonimismo: una práctica por la cual los usuarios son identificados por una dirección o seudónimo, por ejemplo, en un libro mayor visible públicamente.

Seguridad: en las aplicaciones DLT, la seguridad a menudo se refiere a la solidez del consenso, es decir, la confianza en que el libro mayor compartido es preciso.

Contrato inteligente: aplicaciones autoejecutables que pueden desencadenar una acción si se cumplen algunas condiciones preespecificadas.

Stablecoin: una criptomoneda que tiene como objetivo mantener un valor estable en relación con un activo específico, o un grupo o canasta de activos.

Token: una representación digital del valor en un sistema DLT. Se puede decir que los activos que se representan con un token están "tokenizados". (Esto no está relacionado con la distinción entre instrumentos de pago basados en cuentas y basados en tokens).

Depósito tokenizado: una representación digital de un depósito bancario en un sistema DLT. Un depósito tokenizado representa un reclamo en un banco comercial, al igual que un depósito regular.

Valor total bloqueado: valor total de los activos depositados en un protocolo DeFi.

Rendimiento: una medida del número de transacciones que se pueden procesar en un sistema de pago en un período de tiempo determinado, por ejemplo, por segundo.

Validador o nodo validador: una entidad que verifica las transacciones en una cadena de bloques. En algunas redes, este papel es desempeñado por los "mineros".

Prueba de conocimiento cero: una técnica criptográfica que permite a una parte demostrar a otra parte que una declaración es verdadera sin revelar información más allá de ese hecho.