V. Criptomonedas: más allá del fenómeno de moda

Cuando aún no se han cumplido 10 años de su irrupción, las criptomonedas[1] han pasado de ser grandes desconocidas a despertar un notorio interés entre empresas y consumidores, así como bancos centrales y otras autoridades. Llaman la atención porque prometen reemplazar la confianza en instituciones tradicionales, como la banca central y comercial, por una confianza en un nuevo sistema plenamente descentralizado basado en la cadena de bloques (*blockchain*) y la tecnología de registro distribuido (DLT).

El presente capítulo evalúa si las criptomonedas pueden cumplir alguna función como dinero: más allá de ser un fenómeno de moda, ¿qué problemas económicos concretos pueden resolver, en su caso, las criptomonedas actuales? El capítulo repasa primero el contexto histórico. Numerosos episodios de inestabilidad monetaria y monedas fallidas en el pasado ilustran la importancia de los mecanismos institucionales a través de los que se suministra el dinero. Este repaso permite constatar que la esencia del dinero «bueno» ha sido siempre la confianza en la estabilidad de su valor. Para que el dinero pueda hacer honor a su característica definitoria —la capacidad de actuar como un mecanismo de coordinación para facilitar transacciones—, debe poder crecer eficientemente con la economía y suministrarse de forma flexible para responder a fluctuaciones en la demanda. Para ello se precisan determinados mecanismos institucionales —de ahí la creación de los bancos centrales como los conocemos actualmente, con su autonomía y su obligación de rendir cuentas—.

A continuación, el capítulo ofrece una introducción a las criptomonedas y analiza las limitaciones económicas inherentes a la generación descentralizada de confianza que conllevan. Para que la confianza pueda mantenerse, la inmensa mayoría de la potencia computacional debe estar controlada por participantes en la red honestos, todos y cada uno de los usuarios tienen que validar el historial de transacciones y la oferta de la criptomoneda debe estar predeterminada por medio de su protocolo. La confianza puede evaporarse en cualquier momento debido a la fragilidad del procedimiento de consenso descentralizado a través del cual se registran las transacciones. Esto no solo pone en duda la firmeza de cada uno de los pagos, sino que también implica que una criptomoneda puede sencillamente dejar de funcionar, con la consiguiente pérdida de valor total. Es más, incluso si es posible mantener la confianza, la tecnología de las criptomonedas es muy poco eficiente y consume ingentes cantidades de energía. Las criptomonedas no pueden adaptar su oferta a la demanda de transacciones, son proclives a la congestión y su valor experimenta fluctuaciones muy acusadas. En general, la tecnología descentralizada de las criptomonedas constituye, pese a su nivel de sofisticación, un pésimo sustituto del sólido respaldo institucional del dinero.

Con todo, la tecnología subyacente podría ser prometedora para otras aplicaciones, como la simplificación de los procesos administrativos para la liquidación de transacciones financieras. Sin embargo, esta utilidad no ha quedado acreditada todavía. Puesto que las criptomonedas suscitan una miríada de preguntas, el capítulo concluye con un análisis de las respuestas de política, incluida la regulación de los usos privados de la tecnología, las medidas necesarias para evitar abusos y las delicadas cuestiones que pone sobre la mesa la posible emisión de monedas digitales por los bancos centrales.

El auge de las criptomonedas en perspectiva

Una buena manera de determinar si una nueva tecnología puede ser una incorporación realmente útil al panorama monetario actual es volver la vista atrás y hacer inventario de las principales funciones del dinero en una economía y de lo que la historia nos ha enseñado sobre los intentos fallidos de crear nuevas formas privadas de dinero. Después conviene preguntarse si el dinero basado en esta nueva tecnología puede mejorar de alguna forma el panorama monetario actual[2].

Breve historia del dinero

El dinero desempeña una función esencial para facilitar el intercambio económico. Antes de su creación hace varios milenios, los bienes se intercambiaban principalmente por una promesa de devolver el favor en el futuro (intercambio de «pagarés al portador»)[3]. Sin embargo, conforme las sociedades crecieron y la actividad económica se expandió, se hizo más difícil mantener un registro de pagarés cada vez más complejos y los riesgos de incumplimiento y de liquidación comenzaron a ser motivo de preocupación. El dinero y las instituciones que lo emiten se crearon para gestionar esta creciente complejidad y la consiguiente dificultad para mantener la confianza.

El dinero desempeña tres funciones fundamentales y complementarias. Es (i) una unidad de cuenta, una vara de medir que facilita la comparación de precios de las cosas que compramos, así como del valor de las promesas que hacemos; (ii) un medio de cambio: un vendedor lo acepta como medio de pago, con la esperanza de que otra persona se lo acepte a él más adelante; y (iii) un depósito de valor, al permitir que los usuarios transfieran capacidad adquisitiva al futuro[4].

Para cumplir estas funciones, el dinero debe tener idéntico valor en lugares distintos y mantener un valor estable a lo largo del tiempo: decidir si conviene vender un determinado bien o servicio es mucho más fácil si se tiene la seguridad de que la moneda recibida tiene un valor garantizado en términos de su capacidad adquisitiva tanto actual como futura. Una forma de lograr esto es utilizar dinero mercancía puro con un valor intrínseco, como determinadas cantidades de sal o de cereales. Sin embargo, el dinero mercancía, por sí solo, no respalda de forma eficaz el intercambio: puede no estar disponible en todo momento, resulta caro de producir e incómodo de intercambiar y puede ser perecedero[5].

La expansión de la actividad económica hizo necesarias formas de dinero más prácticas que pudieran responder mejor a la creciente demanda, utilizarse de forma más eficiente en el comercio y tener un valor estable. No obstante, el mayor reto ha sido mantener la confianza en los mecanismos institucionales a través de los que se suministra el dinero. En todo el mundo, en contextos y momentos distintos, la emisión de dinero pasó a ser competencia de una autoridad central. Ya en la antigüedad, el sello de un soberano certificaba el valor de una moneda en las transacciones. Más tarde, se crearon las letras de cambio con intermediación bancaria, que permitían a los comerciantes limitar los costes y los riesgos de viajar llevando consigo grandes cantidades de dinero físico[6].

Sin embargo, la experiencia histórica puso de manifiesto igualmente que las monedas cuya oferta es flexible también pueden devaluarse fácilmente[7]. Históricamente, los episodios prolongados de estabilidad de una moneda han sido más la excepción que la regla. De hecho, la confianza se ha perdido con tanta

frecuencia que la historia es un cementerio de monedas. Museos de todo el mundo dedican secciones enteras a este camposanto: por ejemplo, la sala 68 del Museo Británico presenta una muestra de piedras, conchas, tabaco, innumerables monedas y trozos de papel, junto con muchos otros objetos que han acabado allí tras dejar de ser aceptados como medio de cambio. Algunos perecieron a causa de la expansión del comercio y la actividad económica, puesto que se consideraron poco prácticos para un uso a mayor escala. Otros perdieron su vigencia al debilitarse o caer el régimen político que los sostenía. Muchos otros fueron víctimas de la erosión de la confianza en la estabilidad de su valor.

La historia ha demostrado que el dinero puede ser frágil con independencia de que se emita de forma privada, en un contexto competitivo, o lo suministre un emisor soberano monopolista. En el caso del dinero emitido por bancos, su solidez depende por completo de la de los activos que lo respaldan. Los bancos han de transformar riesgos y, por lo tanto, en situaciones extremas, la confianza en el dinero emitido por entidades privadas puede esfumarse de un día para otro. Tampoco han dado siempre buenos resultados los sistemas respaldados por gobiernos, en los que la confianza en el instrumento se asegura de manera centralizada. Más bien al contrario: un ejemplo muy conocido de abuso es la devaluación competitiva de monedas emitidas por príncipes alemanes a principios del siglo XVII, una crisis que se conoce como *Kipper- und Wipperzeit*[8]. Ha habido muchos otros ejemplos, hasta los casos actuales de Venezuela y Zimbabwe. Evitar el uso indebido de las monedas por parte de los emisores soberanos ha sido por tanto una consideración fundamental en el diseño de mecanismos monetarios.

La búsqueda de un marco institucional sólido para la confianza en el dinero culminó con el nacimiento de los bancos centrales actuales. Uno de los primeros pasos en esa dirección fue la creación de bancos comerciales con concesión pública en ciudades-estado europeas durante el periodo entre 1400 y 1600. Estos establecimientos se concibieron para agilizar la actividad comercial proporcionando medios de pago eficientes y de calidad y centralizando una serie de operaciones de compensación y liquidación. Este tipo de bancos, que se constituyeron en polos comerciales como Ámsterdam, Barcelona, Génova, Hamburgo y Venecia, fueron decisivos para estimular el comercio internacional y la actividad económica en general[9]. Con el tiempo, muchos de ellos acabaron funcionando en cierta medida como los actuales bancos centrales. Tal y como los conocemos hoy, los bancos centrales formales también se crearon en muchos casos como respuesta directa a malas experiencias con dinero descentralizado. Por ejemplo, los fracasos de la banca no regulada en Estados Unidos (*wildcat banking*) acabaron por dar lugar al establecimiento del Sistema de la Reserva Federal.

El sistema monetario y de pagos actual

El método probado, seguro y resiliente para generar confianza en el dinero en la época moderna es el banco central independiente. Las características de este sistema son la existencia de objetivos acordados, es decir, objetivos claros de política monetaria y estabilidad financiera; la independencia operativa, administrativa y en la elección de instrumentos de política; y la rendición de cuentas democrática, con el fin de lograr apoyo mayoritario y legitimidad en el plano político. Los bancos centrales independientes han logrado en gran medida el objetivo de proteger el interés económico y político de la sociedad por una moneda estable[10]. En este tipo de sistema, el dinero puede definirse como una «convención social imprescindible

respaldada por una institución estatal que goza de la confianza del público y rinde cuentas por sus actuaciones»[11].

En la práctica totalidad de las economías modernas, el dinero se crea a través de una alianza público-privada entre el banco central y bancos privados, con el primero como piedra angular del sistema. Los depósitos bancarios electrónicos son el principal medio de pago entre usuarios finales, mientras que las reservas en el banco central lo son entre bancos. En este sistema de dos niveles, la confianza se genera a través de bancos centrales independientes y obligados a rendir cuentas, que respaldan las reservas con sus activos y por medio de normas operacionales. Por su parte, la confianza en los depósitos bancarios se genera por varios medios, entre los que se incluyen la regulación, la supervisión y los sistemas de garantía de depósitos, muchos de los cuales emanan en última instancia del Estado.

En cumplimiento de su mandato de mantener una unidad de cuenta y un medio de pago estables, los bancos centrales adoptan un papel activo en la supervisión y la vigilancia de la infraestructura de pagos para su moneda y, en algunos casos, incluso son los proveedores de esa infraestructura. Entre otras obligaciones, los bancos centrales han de cerciorarse de que el sistema de pago funciona correctamente y la oferta de reservas reacciona adecuadamente a los cambios en la demanda, incluso intradía, es decir, deben velar por que la oferta de dinero sea elástica[12].

Gracias a la participación activa de los bancos centrales, los distintos sistemas de pago actuales se caracterizan por su seguridad, eficiencia de costes, escalabilidad y por la confianza en la firmeza de los pagos una vez realizados.

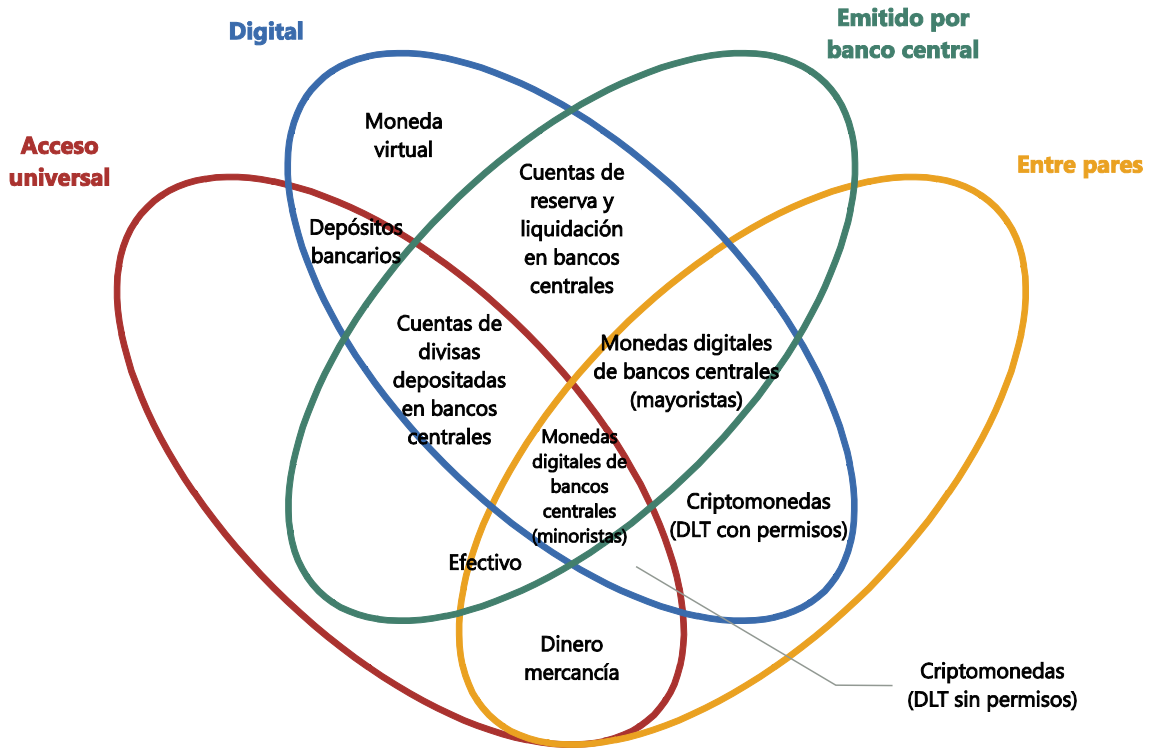
Los sistemas de pago son seguros y eficientes, lo que les permite gestionar volúmenes muy elevados y adaptarse al rápido incremento de los pagos a costes reducidos y sin que se produzca prácticamente ningún uso indebido. Un factor determinante para la seguridad y la eficiencia es la escalabilidad. En las sofisticadas economías actuales, el volumen de pagos es inmenso, equivalente a varias veces el PIB, pero, aun así, el creciente uso del instrumento de pago no se traduce en un incremento proporcional de los costes. Esto es importante, ya que un aspecto fundamental del éxito de cualquier sistema monetario y de pago es el grado de utilización por parte tanto de compradores como de vendedores: cuántos más usuarios se conectan a un sistema de pago concreto, más incentivos tienen para utilizarlo quienes todavía no participan en él.

Los usuarios no solo necesitan tener confianza en el propio dinero, sino que también han de estar seguros de que los pagos se realizarán de forma inmediata y sin contratiempos. Por lo tanto, una característica operacional deseable es la certidumbre del pago («firmeza»), así como otra capacidad relacionada, la de impugnar transacciones que no se han ejecutado correctamente. La firmeza requiere que el sistema esté prácticamente libre de fraude y riesgo operacional, tanto a nivel de las transacciones individuales como del sistema en su conjunto. Una vigilancia estrecha y la rendición de cuentas del banco central contribuyen a sostener la firmeza y, por lo tanto, la confianza.

Aunque hoy en día la mayoría de las transacciones se producen por medios respaldados en última instancia por bancos centrales, a lo largo del tiempo han surgido medios de pago públicos y privados muy variados. La mejor forma de resumirlos es utilizar una taxonomía bautizada como la «flor del dinero» (Gráfico V.1)[13].

La flor del dinero distingue cuatro propiedades esenciales del dinero: el emisor, la forma, el grado de accesibilidad y el mecanismo de transferencia de los pagos. El

La flor del dinero: una taxonomía Gráfico V.1



Fuente: Adaptado de M. Bech y R. Garratt, «Criptomonedas de bancos centrales», *Informe Trimestral del BPI*, septiembre de 2017.

emisor puede ser un banco central, un banco comercial, o incluso nadie, como era el caso cuando se utilizaban mercancías. Su forma puede ser física, como por ejemplo una moneda de metal o un billete de papel, o digital. Además, el dinero puede ser de acceso universal, como los depósitos en bancos comerciales, o de acceso restringido, como las reservas en bancos centrales. La última propiedad es la que se refiere a su mecanismo de transferencia, que puede ser directamente entre las partes (*peer-to-peer*) o a través de un intermediario central, como en el caso de los depósitos. El dinero se basa por lo general en una de estas dos tecnologías básicas: los llamados «*tokens*» (vales o fichas) y las cuentas. El dinero basado en *tokens*, como por ejemplo los billetes bancarios o las monedas físicas, puede intercambiarse directamente entre las partes, pero ese intercambio depende esencialmente de la capacidad del beneficiario para verificar la validez del objeto utilizado para el pago (en el caso del efectivo, el riesgo es la falsificación). En cambio, los sistemas basados en depósitos en cuentas dependen fundamentalmente de la capacidad para verificar la identidad del titular de la cuenta.

Criptomonedas: la elusiva promesa de la confianza descentralizada

¿Cumplen las criptomonedas lo que prometen o acabarán siendo curiosidades efímeras? Para responder a esta pregunta, es necesario definirlas con mayor precisión, entender la tecnología en la que se basan y examinar sus limitaciones económicas.

¿Un pétalo nuevo para la flor del dinero?

Las criptomonedas aspiran a ser una nueva forma de dinero y prometen mantener la confianza en la estabilidad de su valor por medios tecnológicos. Tres son los elementos principales de una criptomoneda. En primer lugar, un conjunto de normas (el «protocolo»), que consiste en código informático que especifica la forma en que pueden realizarse las transacciones. En segundo lugar, un registro contable en el que se deja constancia del historial de transacciones. Y, por último, una red descentralizada de participantes que actualizan, almacenan y comprueban el registro de transacciones con arreglo a las normas del protocolo. Con estos elementos, afirman sus partidarios, una criptomoneda no está sujeta a los incentivos potencialmente espurios de bancos y soberanos.

Atendiendo a la taxonomía de la flor del dinero, las criptomonedas tienen tres características principales. En primer lugar, son digitales, aspiran a ser un medio de pago práctico y utilizan la criptografía para evitar la falsificación y las transacciones fraudulentas. En segundo lugar, aunque se crean de forma privada, no son un pasivo de nadie, puesto que no pueden reembolsarse, y su valor se deriva exclusivamente de las expectativas de que otros continúen aceptándolas. Esto las asimila al dinero mercancía (pese a que carecen de valor intrínseco). Por último, las criptomonedas permiten el intercambio digital directamente entre las partes.

En comparación con otras formas electrónicas de dinero privado, como los depósitos bancarios, el rasgo distintivo de las criptomonedas es el intercambio digital entre pares. Las cuentas bancarias digitales existen desde hace décadas y las «monedas virtuales» de emisión privada (por ejemplo, las que se utilizan en conocidos juegos multijugador en línea como World of Warcraft) nacieron un decenio antes que las criptomonedas. Pero, a diferencia de estos tipos de «dinero», en principio las criptomonedas pueden transferirse a través de un sistema descentralizado sin que sea necesario que una contraparte central ejecute el intercambio.

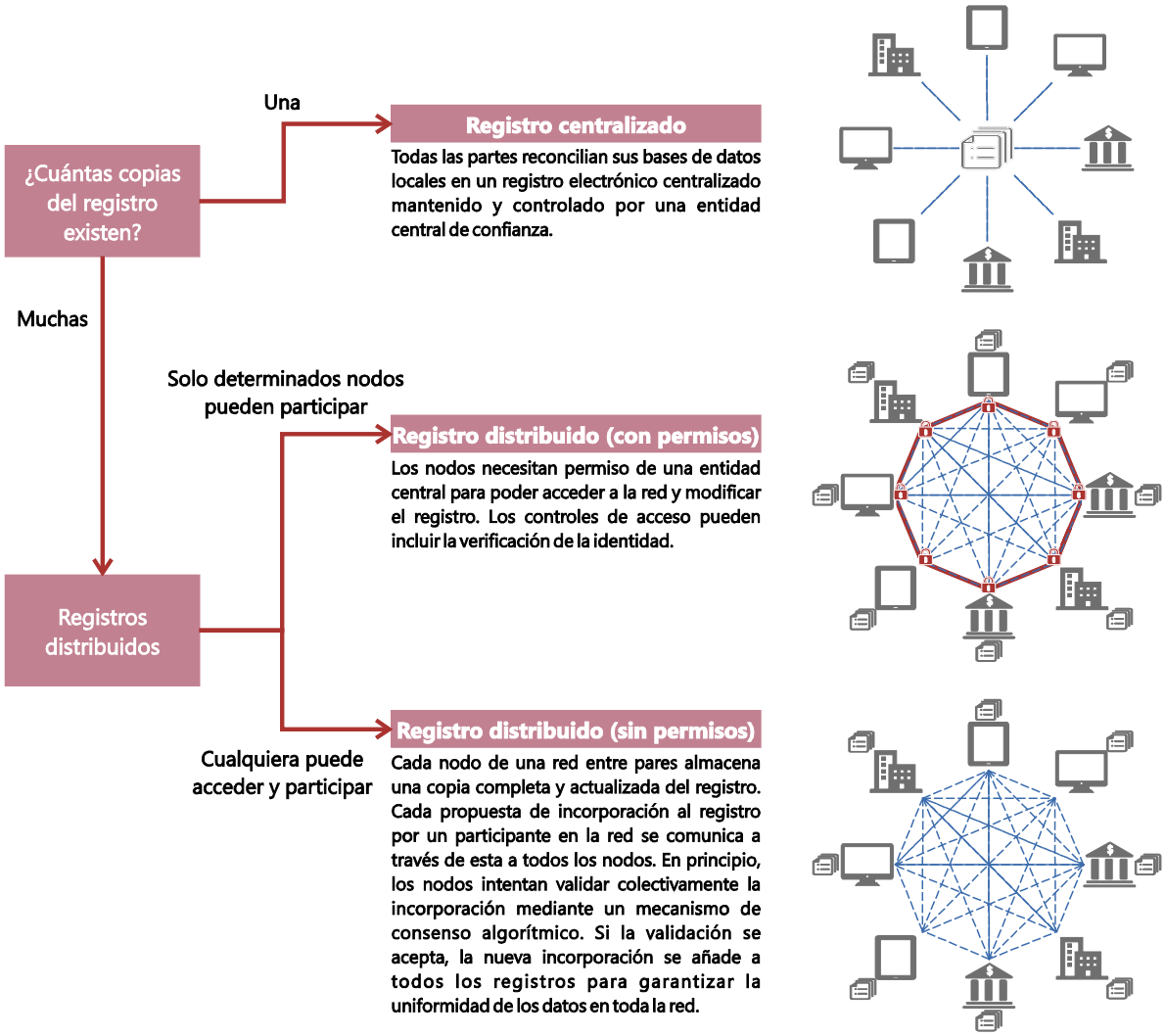
La tecnología de registro distribuido en las criptomonedas

El reto tecnológico de los intercambios digitales entre pares es el denominado «problema del doble gasto». Toda forma de dinero digital es fácilmente replicable, lo que permite que se use fraudulentamente más de una vez. Es más fácil reproducir información digital que falsificar billetes bancarios. En el caso del dinero digital, para resolver el problema del doble gasto se precisa, como mínimo, que alguien lleve un registro de todas las transacciones. Antes de las criptomonedas, la única solución era que un agente centralizado mantuviera ese registro y verificara todas las transacciones.

Las criptomonedas resuelven el problema del doble gasto utilizando un sistema de anotación descentralizado que se conoce como registro distribuido. Ese registro puede ser un archivo (pensemos por ejemplo en una hoja de cálculo de Microsoft Excel) donde se consigna una distribución inicial de criptomonedas y se registra el historial de todas las transacciones posteriores. Cada uno de los usuarios almacena una copia de todo el registro (de ahí la calificación de «distribuido»). Un registro distribuido posibilita el intercambio de dinero digital directamente entre las partes: cada usuario puede comprobar directamente en su copia del registro que una transacción se haya producido y que no haya habido ningún intento de doble gasto[14].

Registro centralizado y registro descentralizado con y sin permisos

Gráfico V.2



		Dinero electrónico privado basado en un sistema fiduciario	Criptomonedas de emisores privados	
			Con permisos	Sin permisos
1	Almacenamiento de saldos/posiciones	Registro (cuentas) almacenado de forma centralizada por bancos y otras instituciones financieras	Almacenamiento descentralizado del registro	
2	Verificación para evitar doble gasto	Concepto basado en la identidad	Concepto entre pares: en el registro distribuido se puede verificar si una unidad específica de una moneda se ha utilizado ya	
3	Procesamiento de transacciones	Actualización de cuentas por el banco	Actualización del registro mediante nodos de confianza	Actualización del registro mediante prueba de trabajo Norma de seguir la cadena más larga
4	Concepto de firmeza/liquidación	Liquidación a través del banco central en última instancia	Liquidación en la propia criptomoneda	Concepto probabilístico de firmeza mediante la norma de seguir la cadena más larga
5	Elasticidad de la oferta	Política del banco central, por ejemplo sobre crédito intradía	El protocolo puede ser modificado por nodos de confianza	Fijada por el protocolo
6	Mecanismos de generación de confianza	Reputación de bancos y bancos centrales, supervisión bancaria, prestamista de última instancia, legislación sobre moneda de curso legal, independencia y obligación de rendir cuentas del banco central, comprobaciones AML/CFT, ciberseguridad	Reputación de la empresa emisora y nodos Nodos de confianza, que pueden estar sujetos a regulación	La prueba de trabajo exige una mayoría computacional honesta

Fuentes: Adaptado de H. Natarajan, S. Krause y H. Gradstein, «Distributed ledger technology (DLT) and blockchain», Grupo del Banco Mundial, *FinTech Note*, nº 1, 2017; BPI.

Aunque todas las criptomonedas se basan en un registro distribuido, difieren en la forma en que se actualiza el registro. Es posible distinguir dos clases principales de criptomonedas, con diferencias sustanciales en su configuración operacional (Gráfico V.2).

La primera se basa en DLT «con permisos» (también denominada «privada»). Este tipo de criptomoneda se asemeja a los mecanismos convencionales de pago en que, para evitar usos indebidos, el registro solo puede ser actualizado por participantes en la criptomoneda autorizados —con frecuencia denominados «nodos» de confianza—. Estos nodos son seleccionados por una autoridad central (por ejemplo, la empresa que ha desarrollado la criptomoneda) y están sujetos a su supervisión. Por lo tanto, aunque las criptomonedas basadas en sistemas con permisos se diferencian del dinero convencional en la forma en que se registran las transacciones (descentralizada frente a centralizada), comparten con él la dependencia de determinadas instituciones como fundamento de la confianza[15].

Una segunda clase de criptomonedas, que se aleja mucho más radicalmente del tradicional sistema de emisión institucional, promete generar confianza en un contexto totalmente descentralizado por medio de DLT «sin permisos» (o «pública»). El registro en el que se deja constancia de las transacciones solo puede modificarse por consenso de los participantes en la moneda: aunque cualquiera puede participar, nadie tiene una clave especial para cambiar el registro.

El concepto de criptomonedas sin permisos se definió, en el caso del Bitcoin[16], en un documento publicado por un programador (o grupo de programadores) anónimo bajo el seudónimo de Satoshi Nakamoto, en el que se proponía una moneda basada en un tipo concreto de registro distribuido, la «cadena de bloques». La cadena de bloques es un registro distribuido que se actualiza en grupos de transacciones denominados «bloques». A continuación los bloques se unen cronológicamente mediante el uso de criptografía para formar la cadena de bloques. Este concepto se ha adaptado para crear innumerables criptomonedas[17].

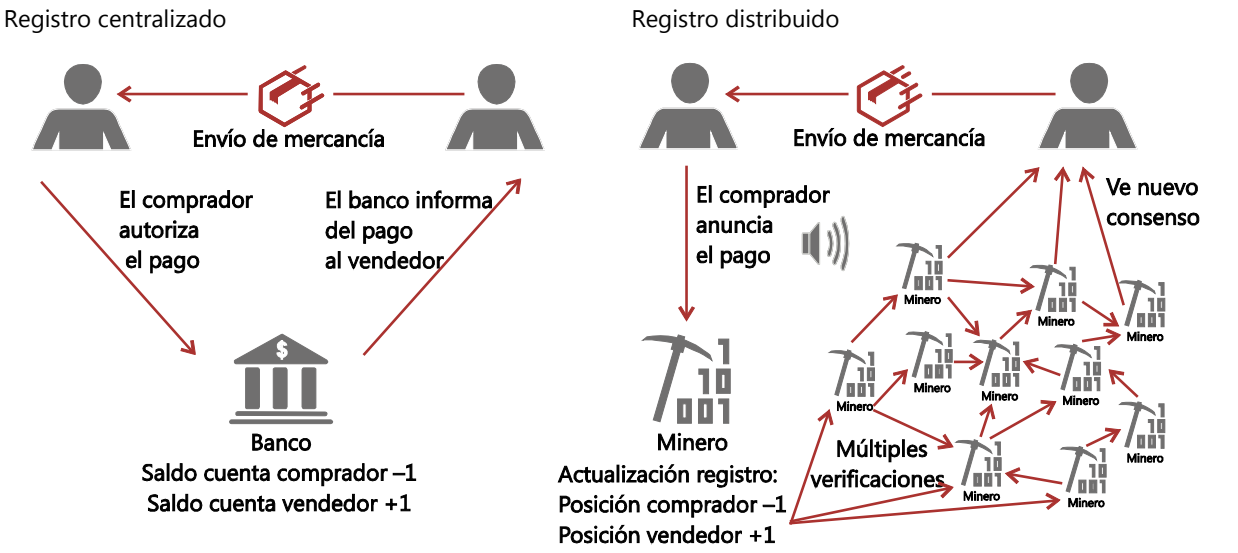
Las criptomonedas basadas en la cadena de bloques sin permisos tienen dos tipos de participantes: los «mineros», que desempeñan la función de agentes de registro, y los «usuarios», que desean realizar transacciones en esa moneda. A primera vista, la idea en la que se basan estas criptomonedas es sencilla: en vez de que un banco registre las transacciones de forma centralizada (Gráfico V.3, panel izquierdo), es un minero el que actualiza el registro y luego todos los usuarios y mineros almacenan la actualización (panel derecho)[18].

La característica fundamental de estas criptomonedas, que sustenta el sistema descrito, es la aplicación de un conjunto de normas (el «protocolo»), concebido para alinear los incentivos de todos los participantes y crear así una tecnología de pago fiable sin un agente de confianza central. El protocolo determina la oferta del activo con el fin de evitar su devaluación —por ejemplo, en el caso del Bitcoin, dicta que no pueden existir más de 21 millones de bitcoins—. Además, el protocolo se diseña para garantizar que todos los participantes cumplan las normas por su propio interés, es decir, generen un equilibrio autosostenible. Los tres aspectos fundamentales en este ámbito se describen a continuación.

En primer lugar, las reglas del juego hacen que la actualización del registro tenga un coste. En la mayoría de los casos, este coste se debe a que para poder introducir modificaciones en el registro se precisa una «prueba de trabajo», una comprobación matemática de que se ha llevado a cabo una determinada cantidad de trabajo informático, que exige a su vez un equipo informático y un consumo eléctrico muy

Transacciones válidas en un registro centralizado/cuenta bancaria y en una criptomoneda sin permisos

Gráfico V.3



Un comprador compra un bien al vendedor, que pone en marcha el envío cuando considera que ha recibido la confirmación del pago. Si el pago se realiza a través de cuentas bancarias —es decir, por medio de un registro centralizado, panel izquierdo—, el comprador da la orden de pago a su banco, que ajusta los saldos cargando a la cuenta del comprador el importe de la transacción y abonándolo en la cuenta del vendedor. A continuación, el banco confirma el pago al vendedor. En cambio, si el pago se lleva a cabo a través de una criptomoneda sin permisos (panel derecho), el comprador primero anuncia públicamente una orden de pago, con arreglo a la cual la cantidad de la criptomoneda que posee el comprador se reduce en una unidad, mientras que la del vendedor se incrementa en una unidad. Después de un tiempo, un minero incluye esta información de pago en una actualización del registro. Posteriormente, el registro actualizado se comparte con otros mineros y usuarios, cada uno de los cuales verifica que la orden de pago recién incorporada no es un intento de doble gasto y ha sido autorizada por el comprador. Luego el vendedor comprueba que el registro que incluye la orden de pago es el que utiliza habitualmente la red de mineros y usuarios.

Fuente: Adaptado de R. Auer, «The mechanics of decentralised trust in Bitcoin and the blockchain», *BIS Working Papers*, próxima publicación.

costosos. Dado que el proceso de prueba de trabajo implica la extracción de cifras mediante laboriosos cálculos, se ha asimilado a la extracción de minerales y suele denominarse «minería»[19]. Como retribución por sus esfuerzos, los mineros perciben una comisión de los usuarios —y, si el protocolo así lo establece, una cantidad de criptomoneda de nueva emisión—.

En segundo lugar, todos los mineros y usuarios de una criptomoneda verifican todas las actualizaciones del registro, lo que induce a los mineros a incluir solo transacciones válidas. Para que una transacción sea válida, debe haber sido iniciada por el propietario de los fondos y no debe ser un intento de doble gasto. Si una actualización del registro incluye una transacción no válida, la red la rechaza y la retribución del minero queda anulada. Por lo tanto, la verificación de todas las actualizaciones del registro por la red de mineros resulta esencial para incentivarles a añadir a la cadena únicamente transacciones válidas[20].

En tercer lugar, el protocolo establece normas para alcanzar un consenso sobre el orden de las actualizaciones del registro. Por lo general, esto se consigue creando incentivos para que, en las actualizaciones, los mineros reconozcan el resultado informático que defiende la mayoría. Esa coordinación es necesaria, por ejemplo, para resolver casos en los que, por retrasos en la comunicación, distintos mineros incorporan actualizaciones contradictorias —actualizaciones que incluyen distintos conjuntos de operaciones (Recuadro V.A.)—.

Con estos ingredientes principales, resulta complicado —aunque no imposible— que una persona falsifique una criptomoneda. Para lograr gastar una criptomoneda dos veces, el falsificador tendría que utilizarla para pagar a un comerciante y generar en secreto una cadena de bloques falsificada en la que no haya constancia de esa transacción. Al recibir la mercancía, el falsificador publicaría la cadena de bloques falsificada, es decir, anularía el pago. Sin embargo, esta cadena de bloques falsificada solo sería la cadena aceptada por la mayoría si fuera más larga que la cadena de bloques que el resto de la red de mineros hubiera producido mientras tanto. Por consiguiente, para que un ataque de gasto doble tenga éxito se precisa un porcentaje significativo de la potencia computacional de la comunidad minera. Dicho de otra forma, como sostenía el documento que acompañó a la creación del Bitcoin, una criptomoneda puede resolver el problema del doble gasto de forma descentralizada únicamente si «nodos honestos controlan la mayoría de la potencia [computacional][21]».

Evaluación de las limitaciones económicas de las criptomonedas basadas en DLT sin permisos

Los partidarios de las criptomonedas como el Bitcoin afirman que estas no solo proporcionan un medio de pago práctico basado en la tecnología digital, sino que también generan un nuevo modelo de confianza. Sin embargo, para que ambas afirmaciones sean ciertas se han de cumplir varias condiciones: que la gran mayoría de la potencia computacional esté controlada por mineros honestos, que los usuarios verifiquen el historial de todas las transacciones y que la oferta de la moneda esté predeterminada por un protocolo. Comprender estas condiciones es importante, porque suscitan dos preguntas básicas sobre la utilidad de las criptomonedas. Primero, ¿va este laborioso proceso de generación de confianza en detrimento de la eficiencia? Segundo, ¿está esa confianza realmente garantizada en todas las circunstancias?

Como implica la primera pregunta, el enorme coste de generar confianza de forma descentralizada constituye una posible limitación clave para la eficiencia. Cabría esperar que los mineros compitan para añadir nuevos bloques al registro mediante la prueba de trabajo solo mientras los beneficios esperados sean mayores que cero[22]. Las instalaciones que utilizan los mineros pueden llegar a albergar potencia computacional equivalente a la de millones de ordenadores personales. En el momento de redactar este Informe, el consumo total de electricidad de la minería de bitcoins equivalía al de economías medianas como Suiza; otras criptomonedas consumen también grandes cantidades de electricidad (Gráfico V.4, panel izquierdo). En pocas palabras, la búsqueda de confianza descentralizada se ha convertido rápidamente en un desastre medioambiental[23].

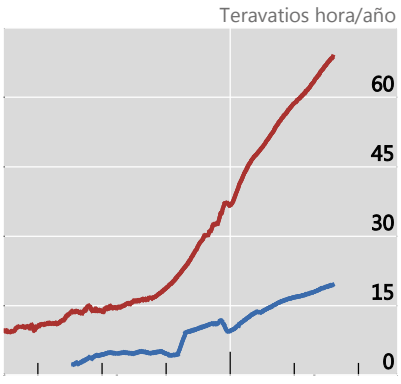
Sin embargo, los problemas económicos subyacentes van mucho más allá del consumo de energía. Están relacionados con la característica definitoria del dinero: la capacidad de promover «externalidades de red» entre los usuarios y servir así de mecanismo de coordinación de la actividad económica. Las criptomonedas presentan deficiencias a este respecto en tres dimensiones: escalabilidad, estabilidad del valor y confianza en la firmeza de los pagos.

En primer lugar, las criptomonedas no pueden aumentar su escala de forma sencilla como sucede con el dinero soberano. Al nivel más básico, para cumplir su promesa de confianza descentralizada, precisan que todos y cada uno de los usuarios descarguen y verifiquen el historial de transacciones en su totalidad, incluida la

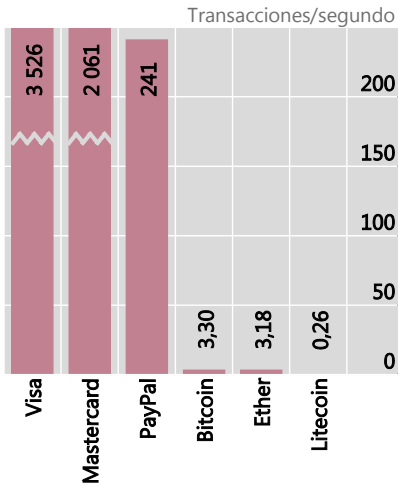
Consumo energético y problemas de escalabilidad

Gráfico V.4

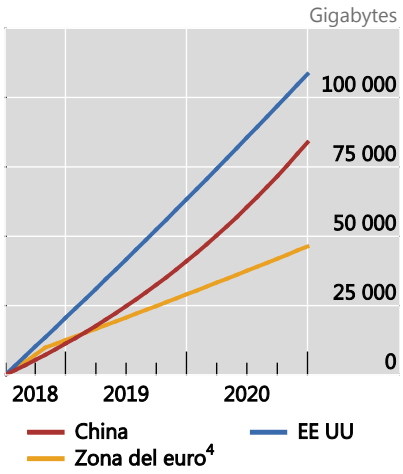
Consumo energético de una selección de criptomonedas[1]



Número de transacciones por segundo[2]



Tamaño hipotético del registro de una criptomoneda para pagos minoristas a escala nacional[3]



[1] Estimación. [2] Datos de 2017. [3] El tamaño hipotético de la cadena de bloques/registro se ha calculado suponiendo que, a partir del 1 de julio de 2018, todas las transacciones minoristas no abonadas en efectivo de China, Estados Unidos o la zona del euro se procesaran por medio de una criptomoneda. Los cálculos se basan en información sobre transacciones no abonadas en efectivo del CPMI (2017) y suponen que con cada transacción se añaden 250 bytes al registro. [4] BE, FR, DE, IT y NL.

Fuentes: Comité de Pagos e Infraestructuras del Mercado, *Statistics on payment, clearing and settlement systems in the CPMI countries*, diciembre de 2017, www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa; cálculos del BPI.

información sobre importes abonados, pagadores y beneficiarios, entre otras. Dado que cada transacción añade cientos de bytes, con el tiempo el tamaño del registro aumenta considerablemente. Por ejemplo, en el momento de redactar este Informe, la cadena de bloques del Bitcoin crecía a un ritmo aproximado de 50 GB anuales y acumulaba ya unos 170 GB. Por ello, para mantener en niveles razonables tanto el tamaño del registro como el tiempo necesario para verificar todas las transacciones (que aumenta con el tamaño del bloque), la capacidad de transacciones de las criptomonedas está limitada estrictamente (Gráfico V.4, panel central).

Un sencillo experimento teórico ilustra la inadecuación de las criptomonedas como medio de pago habitual (Gráfico V.4, panel derecho). Para procesar el número de transacciones digitales minoristas que se tramitan actualmente a través de una selección de sistemas nacionales de pagos minoristas, incluso partiendo de supuestos optimistas, el tamaño del registro se incrementaría hasta superar ampliamente la capacidad de almacenamiento de un *smartphone* medio en apenas unos días, la de un ordenador personal normal en cuestión de semanas y la de los servidores en solo unos meses. Pero el problema no se circunscribe a la capacidad de almacenamiento, sino que afecta también a la de procesamiento: solo las supercomputadoras podrían soportar el ritmo de verificación que impone el flujo de transacciones. Los volúmenes de comunicación asociados podrían paralizar Internet, puesto que millones de usuarios intercambiarían ficheros cuyo tamaño se acercaría a un terabyte.

Otro aspecto del problema de escalabilidad es que la actualización del registro puede congestionarse. Por ejemplo, en el caso de las criptomonedas basadas en la cadena de bloques, solo es posible añadir nuevos bloques al registro a intervalos prefijados, una norma que se ha establecido para limitar el número de transacciones que se incorporan al registro en cada momento. Cuando el elevado número de

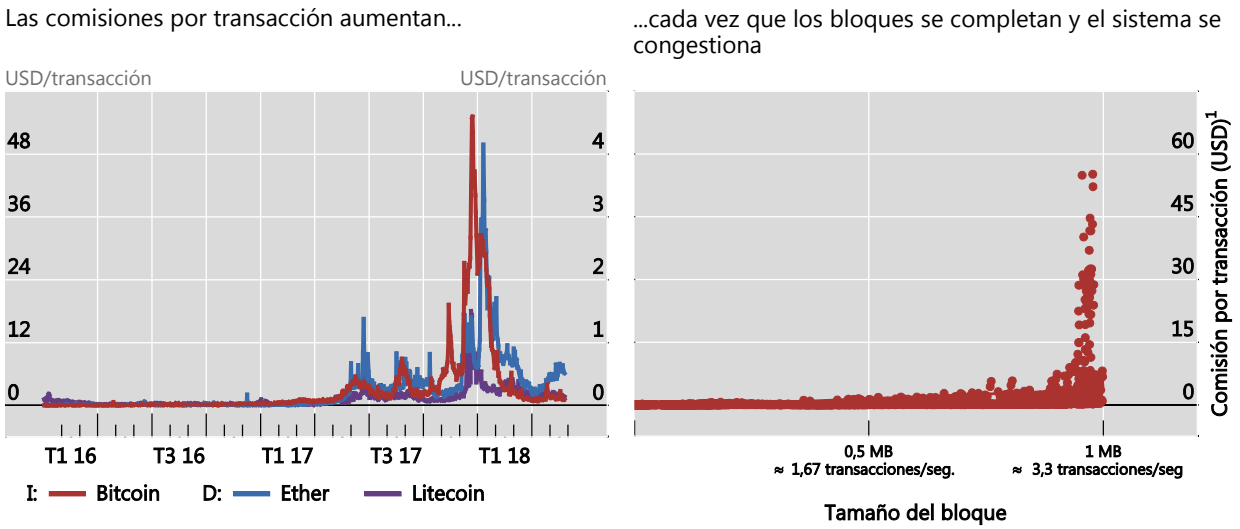
transacciones entrantes hace que los bloques recién incorporados alcancen el tamaño máximo permitido por el protocolo, el sistema se congestiona y muchas transacciones quedan en espera. Al estar limitada la capacidad, las comisiones se disparan cada vez que la demanda de transacciones alcanza dicho límite (Gráfico V.5). Además, en ocasiones las transacciones han permanecido en espera durante varias horas, interrumpiendo el procesamiento de pagos. Esto limita la utilidad de las criptomonedas para las transacciones cotidianas, como el pago de una consumición en una cafetería o de la inscripción en un congreso, por no hablar de los pagos mayoristas[24]. Por lo tanto, cuanta más gente utiliza una criptomoneda, más laboriosos son los pagos. Se incumple así una propiedad esencial del dinero actual: cuantas más personas lo emplean, mayor es el incentivo para usarlo[25].

El segundo problema fundamental de las criptomonedas es la nula estabilidad de su valor, por la ausencia de un emisor centralizado al que se haya encomendado este objetivo. Los bancos centrales bien gestionados consiguen estabilizar el valor interno de su moneda soberana ajustando la oferta de los medios de pago en virtud de la demanda de transacciones. Esto lo hacen con gran frecuencia, en particular durante épocas de tensiones en los mercados, pero también en periodos normales.

En el caso de las criptomonedas, en cambio, para generar cierta confianza en su valor es necesario que un protocolo predetermine la oferta. Esto impide que el suministro sea flexible, por lo que cualquier fluctuación de la demanda provoca cambios en la cotización. Esta es la causa de la extrema volatilidad de las criptomonedas (Gráfico V.6, panel izquierdo). Además, es poco probable que la inestabilidad inherente pueda superarse en su totalidad mejorando los protocolos o mediante ingeniería financiera, como demuestra la experiencia de la criptomoneda Dai. Pese a que se diseñó para que tener un valor fijo de 1 dólar estadounidense, marcó un mínimo de 0,72 dólares tan solo unas semanas después de su lanzamiento a finales de 2017. Otras criptomonedas concebidas para tener un valor estable también han experimentado fluctuaciones de precio considerables (panel central).

Comisiones por transacción a lo largo del tiempo y en relación a la capacidad de transacciones

Gráfico V.5



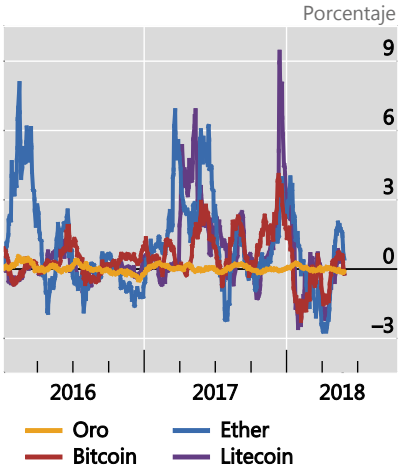
[1] Comisiones por transacción pagadas a mineros durante el periodo entre 1 de agosto de 2010 y 25 de mayo de 2018; promedios diarios.

Fuentes: www.bitinfocharts.com; cálculos del BPI.

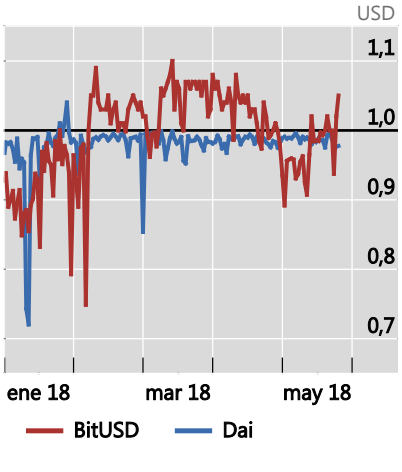
Volatilidad de una muestra de criptomonedas y número de criptomonedas

Gráfico V.6

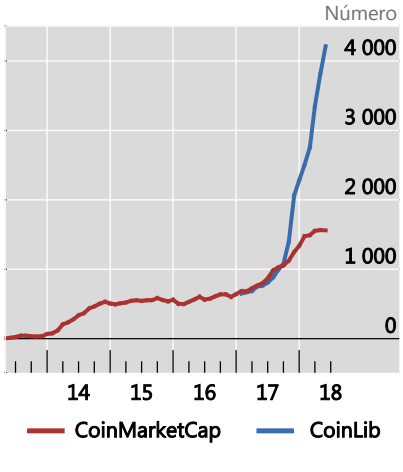
Las principales criptomonedas son comparativamente volátiles[1]



El valor de las «monedas estables» fluctúa[2]



El número de criptomonedas crece rápidamente[3]



[1] Medias móviles de treinta días de rentabilidades diarias. [2] Precio mínimo diario. [3] Basado en el resumen de datos mensuales de dos proveedores. CoinMarketCap incluye solo criptomonedas con un volumen mínimo de negociación en 24 horas de 100 000 USD; CoinLib no aplica ningún umbral mínimo.

Fuentes: www.bitinfocharts.com; www.coinlib.io; www.coinmarketcap.com; Datastream.

Este resultado no es casual. Mantener una oferta de medios de pago ajustada a la demanda de transacciones obliga a tener una autoridad central, por lo general el banco central, que pueda ampliar o contraer su balance. Esta autoridad debe estar dispuesta a tomar posiciones opuestas al mercado en algunas ocasiones, incluso si esto supone asumir riesgos en su balance y absorber pérdidas. En una red descentralizada de usuarios de criptomonedas no existe un agente central que tenga la obligación o incentivos para estabilizar el valor de la moneda: si la demanda de la criptomoneda se reduce, su precio también baja.

Otro factor que contribuye a la inestabilidad de las cotizaciones es la velocidad a la que se crean nuevas criptomonedas —todas las cuales tienden a ser prácticamente intercambiables—. En el momento de elaborar este Informe, existían miles de criptomonedas, aunque esa misma proliferación imposibilita realizar estimaciones fiables de su número exacto (Gráfico V.6, panel derecho). Si recordamos las experiencias de la banca privada en el pasado, la profusión en la emisión de nuevas formas de dinero rara vez genera estabilidad.

El tercer problema pasa por la fragilidad de los cimientos de la confianza en las criptomonedas, tanto en lo que respecta a la firmeza de los pagos como en lo relativo a la confianza en el valor de criptomonedas concretas.

En los sistemas de pago tradicionales, una vez que un pago ha pasado por el sistema nacional y se ha consignado en la contabilidad del banco central, ya no puede revocarse. En cambio, las criptomonedas sin permisos no garantizan la firmeza de los pagos individuales. Uno de los motivos es que, aunque los usuarios pueden verificar la inclusión de una determinada transacción en un registro, pueden convivir versiones distintas del registro sin que ellos lo sepan. Por lo tanto se pueden producir reversiones de transacciones, por ejemplo cuando dos mineros actualicen el registro de manera casi simultánea. Dado que solo una de las dos actualizaciones del registro puede sobrevivir, la firmeza de los pagos realizados en cada una de ellas es probabilística.

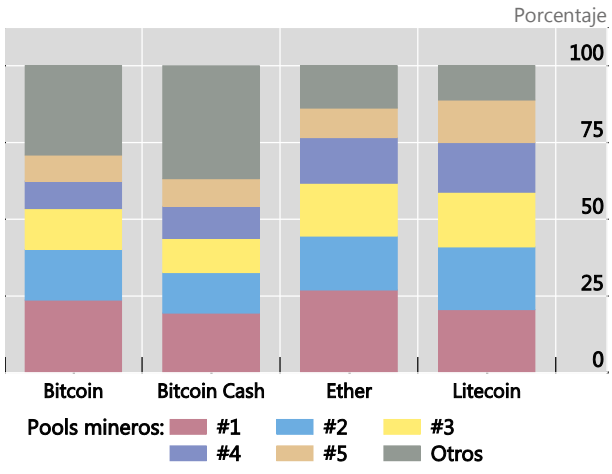
La falta de firmeza de los pagos se ve agravada por el hecho de que las criptomonedas pueden ser manipuladas por un grupo de mineros que controle un porcentaje considerable de la potencia computacional, una posibilidad real dada la concentración que caracteriza a la actividad de minería de muchas criptomonedas (Gráfico V.7, panel izquierdo). Además, no es posible detectar si se está produciendo un ataque estratégico, porque el atacante no revelará el registro (falsificado) hasta estar seguro de su éxito. Por lo tanto, la firmeza nunca estará garantizada. Para las criptomonedas, cada actualización del registro conlleva una prueba de trabajo adicional que un atacante tendría que reproducir. Sin embargo, aunque la probabilidad de que un pago sea firme aumenta con las posteriores actualizaciones del registro, nunca alcanza el 100%[26].

No solo resulta incierta la confianza en la firmeza de los pagos, sino que la confianza en las distintas criptomonedas en sí también carece de cimientos sólidos. El motivo es un fenómeno denominado bifurcación («*forking*»). Se trata de un proceso por el que un subconjunto de titulares de una criptomoneda se coordinan para usar una nueva versión del registro y protocolo, mientras que otros continúan usando el registro original. De esta forma, una criptomoneda puede dividirse en dos subredes de usuarios. Aunque hay muchos ejemplos recientes, el episodio del 11 de marzo de 2013 resulta especialmente llamativo porque —contradiciendo la idea de alcanzar la confianza por medios descentralizados— se solucionó mediante la coordinación centralizada de los mineros. Aquel día, una actualización errónea del software dio lugar a incompatibilidades entre una parte de la red de Bitcoin, que continuó extrayendo por medio del protocolo anterior, y otra parte que comenzó a utilizar un protocolo actualizado. Durante varias horas fueron creciendo dos cadenas de bloques diferentes. En cuanto se conoció esta bifurcación, el bitcoin perdió más de un tercio de su valor (Gráfico V.7, panel derecho). La bifurcación se subsanó finalmente mediante la acción coordinada de los mineros, que dejaron de aplicar temporalmente el protocolo e ignoraron la cadena más larga. Sin embargo, muchas transacciones se anularon horas después de que los usuarios las creyeran firmes. Este

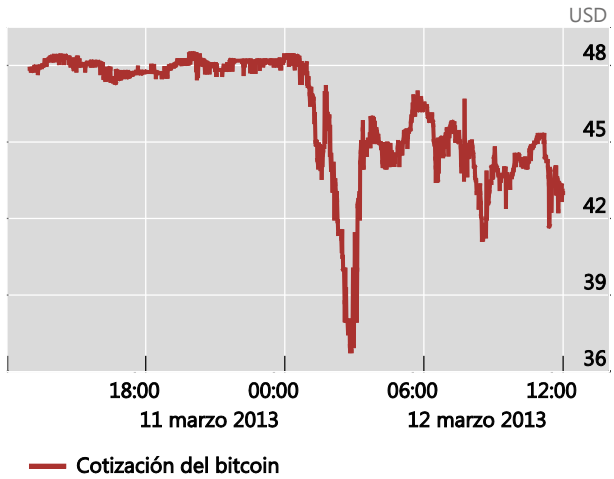
Concentración de la minería y valor del bitcoin durante una bifurcación temporal

Gráfico V.7

Elevada concentración de la minería de todas las criptomonedas[1]



Valor del bitcoin durante una bifurcación temporal en 2013[2]



[1] Datos de los mayores *pools* de mineros a 28 de mayo de 2018. [2] Evolución de la cotización del bitcoin durante su bifurcación el 11 y 12 de marzo de 2013.

Fuentes: www.btc.com; www.cash.coin.dance; CoinDesk; www.etherchain.org ; www.litecoinpool.org.

episodio demuestra hasta qué punto es fácil que las criptomonedas se bifurquen, lo que da lugar a considerables pérdidas en la cotización.

Otro aspecto aún más preocupante que subyace a estos episodios es que la bifurcación podría ser un síntoma de una deficiencia fundamental: la fragilidad del consenso descentralizado que se precisa para actualizar el registro y, con él, de la propia confianza en la criptomoneda. El análisis teórico (Recuadro V.A) sugiere que esa coordinación en la actualización del registro podría romperse en cualquier momento, lo que se traduciría en la pérdida completa de valor.

En términos generales, las criptomonedas descentralizadas presentan varias deficiencias. Las más importantes se derivan del grado extremo de descentralización: generar la necesaria confianza en ese tipo de sistema obliga a un enorme dispendio de potencia computacional, el almacenamiento descentralizado de un registro de transacciones es ineficiente y el consenso descentralizado es vulnerable. Algunos de estos problemas podrían solucionarse mediante nuevos protocolos y otros avances[27], pero otros parecen inherentes a la fragilidad y la limitada escalabilidad de este tipo de sistemas descentralizados. En última instancia, esto podría indicar que la deficiencia fundamental de las criptomonedas es la inexistencia de un mecanismo institucional adecuado a escala nacional.

Más allá de la burbuja: uso de la tecnología de registro distribuido

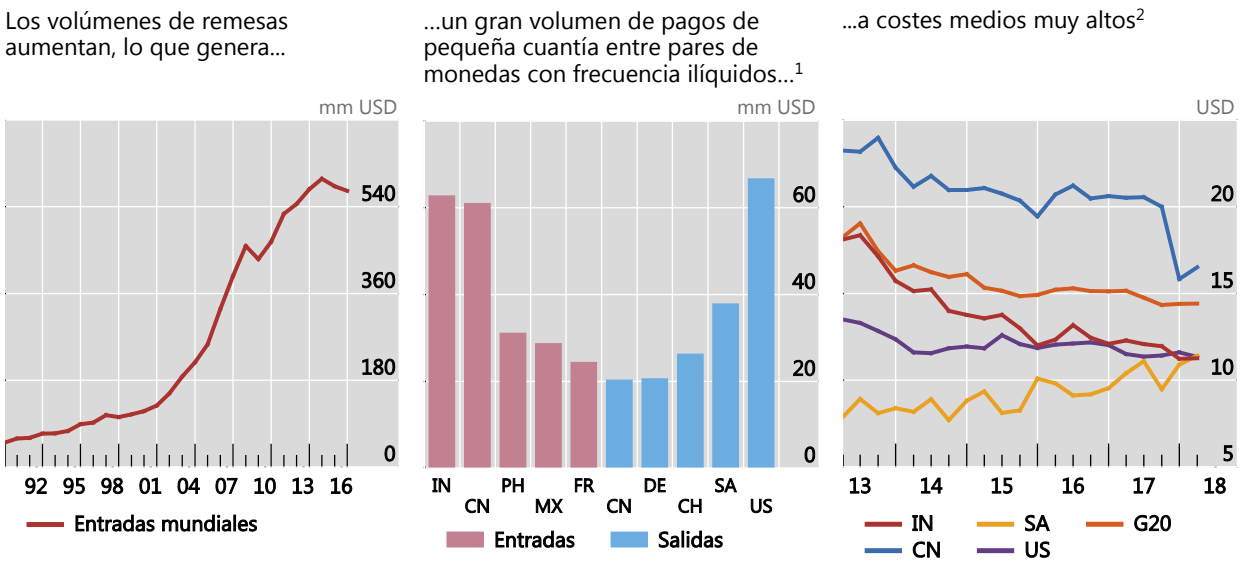
Aunque las criptomonedas no funcionan bien como dinero, la tecnología subyacente sí parece prometedora para otros ámbitos. Un ejemplo notable es el de los servicios de pagos transfronterizos de pequeña cuantía. En términos más generales, si se compara con las soluciones tecnológicas centralizadas más comunes, la DLT puede ser eficiente cuando las ventajas del acceso descentralizado superan a los inconvenientes del mayor coste operativo que conlleva mantener múltiples copias del registro.

Obviamente, ese tipo de soluciones de pago presentan diferencias fundamentales con las criptomonedas. Un ejemplo reciente de esta tecnología en un proyecto sin ánimo de lucro es el sistema basado en la cadena de bloques «Building Blocks» del Programa Mundial de Alimentos, que gestiona los pagos de ayuda alimentaria destinados a refugiados sirios en Jordania. La unidad de cuenta y, en última instancia, el medio de pago de esta plataforma es la moneda soberana, por lo que se trata de un sistema de «criptopagos», pero no de una criptomoneda. Además, Building Blocks está bajo el control centralizado del Programa Mundial de Alimentos, y por una buena razón: las transacciones realizadas en el marco de un experimento inicial basado en el protocolo sin permisos de Ethereum resultaron lentas y costosas. El sistema se rediseñó entonces para utilizar una versión con permisos de dicho protocolo, lo que permitió reducir los costes por transacción en aproximadamente el 98% frente a las alternativas basadas en servicios bancarios[28].

Los sistemas de criptopagos con permisos también pueden resultar prometedores para las transferencias transfronterizas de pequeña cuantía, que son importantes para los países con gran parte de su población activa en el extranjero. Los flujos de remesas mundiales superan los 540 000 millones de dólares anuales (Gráfico V.8, paneles izquierdo y central). Los sistemas de pagos internacionales actuales cuentan con múltiples intermediarios, lo que eleva notablemente sus costes (panel derecho). Dicho esto, aunque los sistemas de criptopagos son una opción para responder a esas necesidades, también se están considerando otras tecnologías y todavía no está claro cuál es más eficiente.

Indicadores del volumen y el coste de las remesas

Gráfico V.8



[1] Datos de 2016. [2] Coste medio total de enviar 200 USD con todos los proveedores de servicios de remesas del mundo. Para CN e IN, coste total medio del país receptor; para el G20, SA y US, coste total medio del país remitente.

Fuentes: Banco Mundial, *Remittance Prices Worldwide*, remittanceprices.worldbank.org; Banco Mundial; cálculos del BPI.

Previsiblemente, los usos más relevantes combinarán los criptopagos con sofisticados códigos autoejecutables y sistemas de autorización de datos. Algunos protocolos de criptomonedas descentralizadas como Ethereum permiten ya la utilización de contratos inteligentes que ejecutan automáticamente los flujos de pagos de derivados. Por el momento, su eficacia es limitada debido a la escasa liquidez y las deficiencias intrínsecas de las criptomonedas sin permisos. Sin embargo, la tecnología subyacente puede ser adoptada por plataformas de intercambio registradas, que la aplicarían por medio de protocolos con permisos que utilizan la moneda soberana como respaldo, lo que permitiría simplificar la ejecución de la liquidación. El valor añadido de la tecnología probablemente vendrá dado por la simplificación de los procesos administrativos relacionados con transacciones financieras complejas, como la financiación del comercio (Recuadro V.B). Lo más importante, sin embargo, es que ninguna de estas aplicaciones precisa el uso o la creación de una criptomoneda.

Implicaciones para las políticas económicas

El auge de las criptomonedas y la tecnología relacionada pone sobre la mesa una serie de cuestiones relativas a las políticas económicas. Las autoridades están buscando fórmulas para garantizar la integridad de los mercados y los sistemas de pago, proteger a consumidores e inversores y salvaguardar la estabilidad financiera general. La lucha contra el uso ilícito del dinero es un desafío considerable. Al mismo tiempo, las autoridades quieren preservar los incentivos a largo plazo para la innovación y, sobre todo, respetar en todo momento el principio de «a igual riesgo, igual regulación»[29]. Estos objetivos son en su mayoría recurrentes, pero las criptomonedas generan nuevos retos y pueden obligar a las autoridades a adoptar

nuevos enfoques y utilizar herramientas novedosas. Una cuestión relacionada es si los bancos centrales deberían emitir sus propias monedas digitales (CBDC).

Retos reguladores de las criptomonedas

Un primer reto clave para la regulación es el de la lucha contra el blanqueo de capitales (AML) y la financiación del terrorismo (CFT). La cuestión es si el auge de las criptomonedas ha permitido eludir determinadas medidas AML/CFT, como las normas «conozca a su cliente» (KYC), y en qué medida. Como consecuencia del carácter anónimo de las criptomonedas, resulta complicado determinar hasta qué punto se utilizan para evadir impuestos o controles de capital o para operaciones ilegales en general. Sin embargo, hechos como la fuerte reacción del bitcoin en el mercado tras el cierre de Silk Road, un importante mercado de drogas ilegales, sugieren que una considerable parte de la demanda de criptomonedas procede de actividades ilícitas (Gráfico V.9, panel izquierdo)[30].

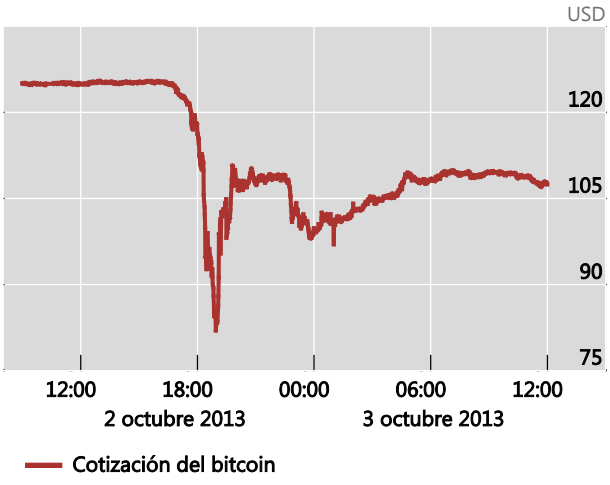
Un segundo desafío engloba las normas sobre valores y otras regulaciones que protegen a consumidores y usuarios. Un problema habitual es el robo digital. Dado que los registros distribuidos son muy voluminosos y los costes de transacción son elevados, la mayoría de los usuarios acceden a sus posiciones en criptomonedas a través de terceros, como proveedores de «criptomonederos» (*wallets*) o plataformas de intercambio de criptomonedas. Paradójicamente —y en contraste absoluto con la promesa inicial del Bitcoin y de otras criptomonedas—, muchos usuarios que recurrieron a estos activos por su desconfianza en bancos y gobiernos han acabado confiando en intermediarios no regulados. Algunos de ellos, como Mt Gox o Bitfinex, han resultado ser fraudulentos o han sido víctimas de ataques informáticos[31].

El fraude es también un problema grave en las ofertas iniciales de criptomonedas (OIC). Una OIC consiste en la subasta pública de una cantidad inicial de criptomonedas y en ocasiones otorga a los compradores derechos de participación

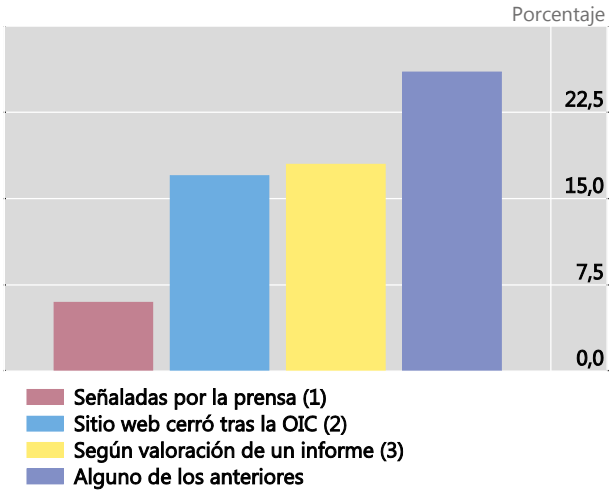
El cierre de un mercado ilegal y la legitimidad de las OIC

Gráfico V.9

Fuerte reacción de las criptomonedas a los cierres de mercados ilegales[1]



Un elevado porcentaje de las OIC podrían ser fraudulentas



[1] Cotización del bitcoin durante el cierre de Silk Road en octubre de 2013.

Fuentes: C. Catalini, J. Boslego y K. Zhang, «Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings», *MIT Working Papers*, próxima publicación; CoinDesk.

en una sociedad «*start-up*». Haciendo caso omiso de las advertencias de las autoridades, los inversores han acudido en masa a las OIC, pese a que con frecuencia están vinculadas a proyectos empresariales opacos sobre los que se ofrece información escasa y no auditada. Muchos de estos proyectos han resultado ser esquemas piramidales fraudulentos (Gráfico V.9, panel derecho).

Un tercer reto, en este caso a más largo plazo, se refiere a la estabilidad del sistema financiero. Está por ver si el uso generalizado de criptomonedas y productos financieros de ejecución automática relacionados genera nuevas vulnerabilidades financieras y riesgos sistémicos. Será imprescindible seguir muy de cerca los acontecimientos. Además, dados sus novedosos perfiles de riesgo, estas tecnologías obligan a mejorar la capacidad de reguladores y organismos supervisores. En algunos casos, por ejemplo en la ejecución de pagos de gran volumen y elevada cuantía, el perímetro regulador puede tener que ampliarse para incluir a entidades que utilizan tecnologías nuevas, a fin de evitar la acumulación de riesgos sistémicos.

Los reguladores de todo el mundo son plenamente conscientes de la necesidad de reforzar la nueva regulación y la vigilancia de las criptomonedas y los criptoactivos relacionados. En particular, un reciente Comunicado de los Ministros de Finanzas y Gobernadores de Bancos Centrales del G-20 destaca problemas relacionados con la protección de consumidores e inversores, la integridad del mercado, la evasión fiscal y las normas AML/CFT, por lo que reclama la vigilancia continua por parte de los organismos normalizadores internacionales. Asimismo, insta al Grupo de Acción Financiera a avanzar en la implantación mundial de normas pertinentes[32].

Sin embargo, el diseño y la implantación efectiva de la normativa reforzada no están exentos de dificultades. Las definiciones jurídicas y reguladoras no siempre se ajustan a las nuevas realidades. Las tecnologías se utilizan para múltiples actividades económicas, que en muchos casos están reguladas por distintos organismos supervisores. Por ejemplo, empresas tecnológicas están utilizando actualmente OIC para recaudar fondos para proyectos no relacionados en absoluto con las criptomonedas. Dejando a un lado las diferencias semánticas —se subastan monedas en lugar de acciones—, estas OIC se asemejan a las ofertas públicas iniciales (OPI) en las bolsas tradicionales, así que lo natural sería que los organismos que regulan los mercados de valores les aplicaran políticas de regulación y supervisión similares. Sin embargo, algunas OIC también han incluido la subasta de fichas servicio o «*utility tokens*», que prometen el acceso futuro a *software* como por ejemplo juegos. Esta característica no constituye una actividad de inversión, sino que requeriría la aplicación de leyes de protección del consumidor por parte de los organismos competentes[33].

En términos operacionales, la principal dificultad radica en que las criptomonedas basadas en un sistema descentralizado sin permisos no encajan bien en los marcos actualmente en vigor. En particular, carecen de una identidad jurídica que pueda insertarse en el perímetro regulador. Las criptomonedas residen en su propio entorno digital sin fronteras nacionales y en general pueden funcionar al margen del marco institucional vigente o de cualquier otra infraestructura. Su domicilio jurídico —si lo tienen— puede estar en un centro extraterritorial o ser imposible de determinar con precisión. Por lo tanto, solo pueden regularse por cauces indirectos.

¿Cómo pueden las autoridades articular un enfoque regulador? Hay tres consideraciones importantes.

La primera, que el auge de las criptomonedas y los criptoactivos obliga a reajustar el perímetro regulador. Las nuevas fronteras deben reflejar una nueva realidad en la que cada vez es más difusa la demarcación de responsabilidades de los distintos reguladores dentro de cada jurisdicción y entre ellas[34]. Habida cuenta del carácter global de las criptomonedas, solo una regulación coordinada a escala mundial puede ser eficaz[35].

La segunda consideración es la posible regulación de la interoperabilidad de las criptomonedas con entidades financieras reguladas. Los mercados regulados son los únicos que pueden proporcionar la liquidez necesaria para que los productos financieros basados en DLT sean algo más que mercados nicho, y los flujos de liquidación deben convertirse en última instancia en moneda soberana. Por lo tanto, se podrían adaptar las normas fiscales y de capital para instituciones reguladas que deseen operar con activos relacionados con criptomonedas. Los reguladores podrían vigilar si los bancos entregan o reciben criptomonedas como colateral, y cómo lo hacen.

La tercera consideración pasa por regular las instituciones que ofrecen servicios relacionados específicamente con criptomonedas. Por ejemplo, para garantizar el cumplimiento efectivo de las normas AML/CFT, la regulación podría centrarse en el punto en el que la criptomoneda se convierte en la moneda nacional. Otras leyes y regulaciones vigentes en materia de servicios de pago se centran en la seguridad, la eficiencia y la legalidad del uso, principios que podrían aplicarse también a los proveedores de infraestructuras de criptomonedas, como los *wallets*[36]. Para evitar fugas, idealmente la regulación debería ser bastante similar y aplicarse de forma uniforme en las distintas jurisdicciones.

¿Deberían emitir los bancos centrales sus propias monedas digitales?

Una cuestión a medio plazo relacionada con las políticas es la posible emisión de monedas digitales de bancos centrales (CBDC), incluyendo quién debería tener acceso a ellas. Las CBDC funcionarían en gran medida como el efectivo: en primera instancia, sería el banco central el que emitiría una CBDC, pero después esta circularía entre bancos, sociedades no financieras y consumidores sin la intervención del banco central[37]. Una CBDC podría intercambiarse bilateralmente entre participantes del sector privado por medio de registros distribuidos, sin necesidad de que el banco central llevase un control ni ajustara los saldos. La moneda digital se basaría en un registro distribuido con permisos (Gráfico V.2) y el banco central sería el encargado de determinar quién actúa como nodo de confianza.

Aunque la distinción entre CBDC para uso general y los actuales pasivos digitales de bancos centrales —los saldos de reservas de bancos comerciales— puede antojarse meramente técnica, en realidad se trata de una diferencia fundamental en cuanto a sus repercusiones para el sistema financiero. Una CBDC para uso general —emitida para consumidores y empresas— podría afectar profundamente a tres ámbitos de actuación principales de los bancos centrales: los pagos, la estabilidad financiera y la política monetaria. Un reciente informe conjunto del Comité de Pagos e Infraestructuras del Mercado y el Comité de los Mercados analiza las consideraciones subyacentes[38] y llega a la conclusión de que las ventajas y desventajas de una CBDC para uso general dependerían de sus características de diseño específicas. El informe señala que, aunque todavía no han surgido aspirantes de peso, un instrumento de ese tipo traería consigo considerables vulnerabilidades financieras, mientras que sus beneficios están menos claros.

Por el momento, los bancos centrales vigilan de cerca las tecnologías y afrontan con cautela la cuestión de la implementación. Algunos están evaluando las ventajas e inconvenientes de emitir CBDC muy específicas, cuyo uso estaría restringido a operaciones mayoristas entre instituciones financieras. Este tipo de monedas no pondrían en peligro el actual sistema de dos niveles, sino que estarían concebidas para mejorar la eficiencia operativa de los mecanismos actuales. Hasta ahora, sin embargo, los experimentos realizados con CBDC mayoristas no justifican claramente su emisión inmediata (Recuadro V.C).

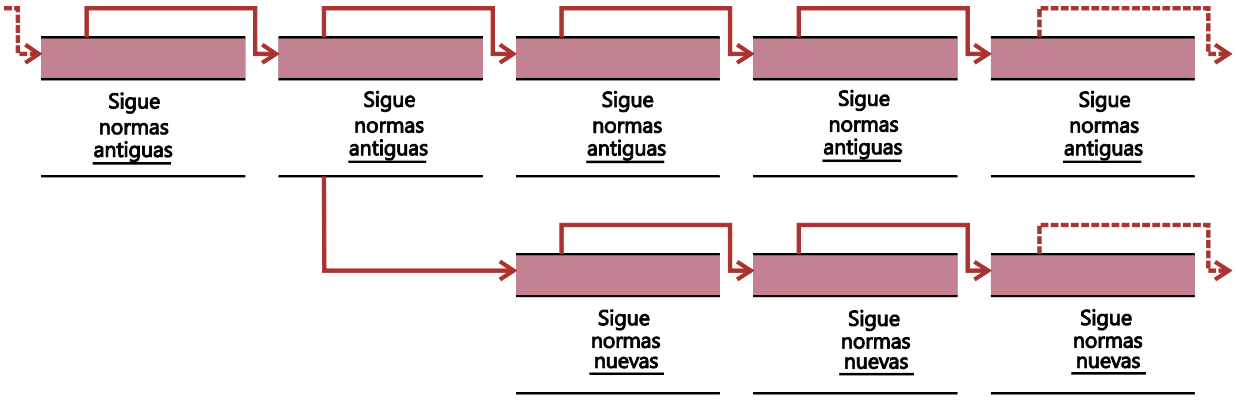
Recuadro V.A

La bifurcación y la inestabilidad del consenso descentralizado en la cadena de bloques

La bifurcación (*forking*) ha contribuido al crecimiento exponencial del número de criptomonedas (Gráfico V.6, panel derecho). Por ejemplo, solo en enero de 2018 se produjeron las bifurcaciones Bitcoin ALL, Bitcoin Cash Plus, Bitcoin Smart, Bitcoin Interest, Quantum Bitcoin, BitcoinLite, Bitcoin Ore, Bitcoin Private, Bitcoin Atom y Bitcoin Pizza. Estas bifurcaciones pueden producirse de formas muy distintas, algunas permanentes y otras temporales. Por ejemplo, la denominada «bifurcación dura» (Gráfico V.A) se produce cuando parte de los mineros de una criptomoneda se coordinan para cambiar el protocolo, adoptando un nuevo conjunto de normas incompatible con el anterior. Los cambios pueden afectar a muchos aspectos del nuevo protocolo, como el tamaño máximo permitido de los bloques, la frecuencia con que se pueden incorporar bloques a la cadena o la prueba de trabajo necesaria para actualizarla. Los mineros que adoptan el nuevo protocolo parten de la antigua cadena de bloques, pero después incorporan bloques que no reconocen los mineros que no han hecho el cambio. Estos continúan alargando la cadena de bloques aplicando las normas antiguas, de manera que van creciendo dos cadenas de bloques independientes, cada una con su propio historial de transacciones.

Ejemplo de una bifurcación dura

Gráfico V.A



Fuente: BPI.

Las bifurcaciones frecuentes pueden ser sintomáticas de un problema inherente al método por el que se forja el consenso en la red descentralizada de mineros de una criptomoneda. El problema económico subyacente es que este consenso descentralizado no es único. La norma de seguir la cadena más larga incentiva a los mineros a seguir a la mayoría computacional, pero no establece de forma inequívoca hacia dónde debe dirigirse esa mayoría. Por ejemplo, si un minero considera que la última actualización del registro va a ser ignorada por el resto de la red, su estrategia óptima sería ignorar también dicha actualización. Y si la mayoría de mineros se coordina para ignorar una actualización, efectivamente esto pasa a ser el nuevo equilibrio. De este modo, pueden surgir así equilibrios arbitrarios —como ha ocurrido con frecuencia, tal y como atestiguan los episodios de bifurcación y los miles de bloques «huérfanos» (Bitcoin) o bloques «tíos» (Ethereum) que se han anulado retroactivamente—. En lo que respecta a la solidez de la actualización descentralizada de la cadena de bloques, preocupan también los incentivos de los mineros para bifurcar la cadena por razones estratégicas cuando el último bloque añadido por otro minero incluya comisiones por transacción elevadas que puedan desviarse anulando ese bloque por medio de una bifurcación①.

① Véase un análisis de las particularidades de la actualización de la cadena de bloques en B. Biais, C. Bisière, M. Bouvard y C. Casamatta, «The blockchain folk theorem», *TSE Working Papers*, nº 17–817, 2017. Para un análisis de las razones estratégicas para crear una bifurcación, véase M. Carlsten, H. Kalodner, S. M. Weinberg y A. Narayanan, «On the instability of bitcoin without the block reward». *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.

Recuadro V.B

La tecnología de registro distribuido en la financiación del comercio

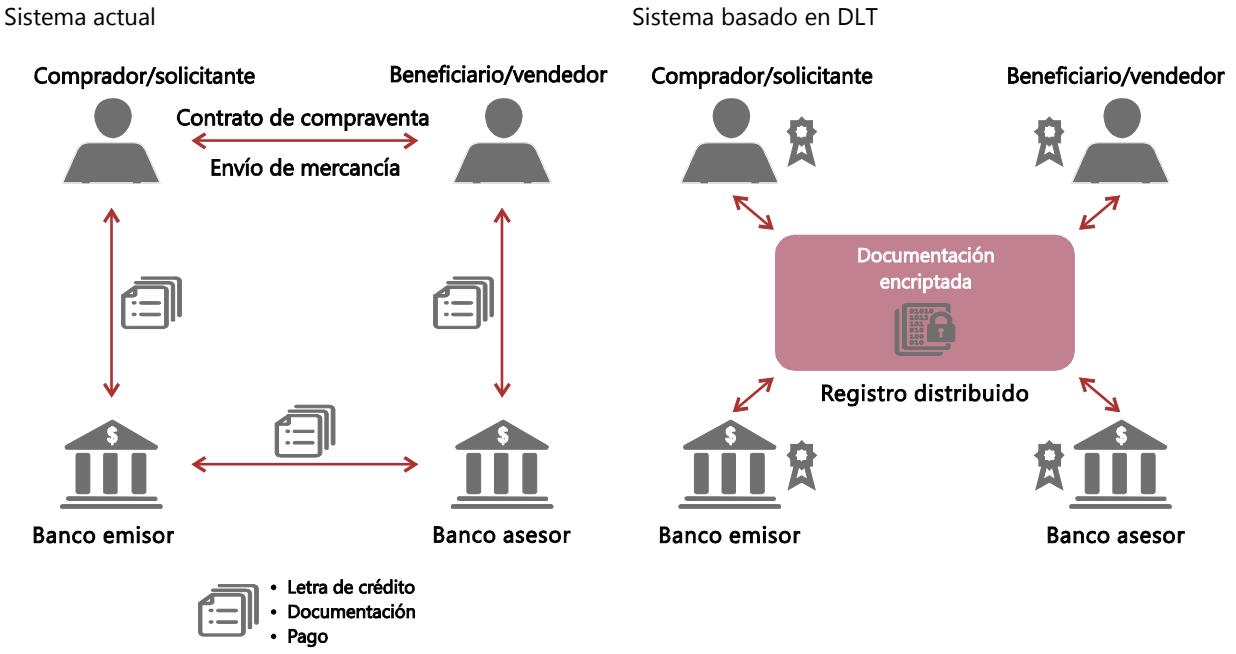
La Organización Mundial del Comercio estima que entre el 80% y el 90% del comercio mundial depende de la financiación de las operaciones comerciales. Cuando un exportador y un importador llegan a un acuerdo para comerciar, el exportador suele preferir cobrar por adelantado ante el riesgo de que el importador no realice el pago una vez reciba las mercancías. A su vez, el importador prefiere reducir su propio riesgo exigiendo una prueba documental de que las mercancías se han expedido antes de realizar el pago inicial.

La financiación del comercio que ofrecen los bancos y otras entidades financieras se ha concebido para tender un puente entre las necesidades de ambas partes. Lo habitual es que un banco con domicilio en el país de origen del importador emita una carta de crédito por la que garantiza el pago al exportador, previa recepción de documentación acreditativa del envío, como un conocimiento de embarque. A su vez, un banco domiciliado en el país del exportador podría conceder a este un crédito con dicha garantía y luego cobraría el pago al banco del importador para completar la transacción.

En su forma actual (Gráfico V.B, panel izquierdo), la financiación del comercio resulta engorrosa, compleja y cara. Conlleva gran número de intercambios documentales entre el exportador, el importador, sus respectivas entidades bancarias y los agentes que realizan las comprobaciones físicas de las mercancías enviadas en cada punto de control, así como agencias de aduanas, agencias de crédito a la exportación públicas y compañías de seguros de transporte. A menudo, el proceso exige realizar tareas administrativas en papel. La DLT puede simplificar la ejecución de los contratos subyacentes (panel derecho). Por ejemplo, el uso de un contrato inteligente podría liberar automáticamente el pago al exportador en cuanto se incorpore al registro la validación del envío. Además, la mayor disponibilidad de información sobre qué envíos ya se han financiado podría reducir también el riesgo de que los exportadores obtengan ilegalmente créditos de distintos bancos para el mismo envío.

Funcionamiento de la financiación del comercio con un registro distribuido

Gráfico V.B



Fuente: Adaptado de www.virtusapolaris.com.

Recuadro V.C

Monedas digitales mayoristas emitidas por bancos centrales

Durante las últimas décadas, los bancos centrales han apostado por las tecnologías digitales para mejorar la eficiencia y la solidez de los pagos y del sistema financiero en su conjunto. La tecnología digital les ha permitido economizar en la provisión de liquidez a los sistemas de liquidación bruta en tiempo real (RTGS). Enlazando estos sistemas por medio de *Continuous Linked Settlement* (CLS), bancos comerciales de todo el mundo liquidan billones de dólares en divisas a diario. El sistema CLS contribuye a eliminar el riesgo «Herstatt», es decir, el riesgo de que un banco corresponsal en una transacción en moneda extranjera tenga problemas financieros antes de pagar el contravalor al destinatario designado. Este riesgo solía constituir una amenaza considerable para la estabilidad financiera. Más recientemente, se han generalizado pagos minoristas más rápidos en todo el mundo y los bancos centrales promueven y facilitan activamente esta tendencia.

En el marco de sus incursiones generales en nuevas tecnologías de pago, los bancos centrales también están experimentando con sus propias monedas digitales (CBDC) mayoristas. En este caso, se trata de versiones basadas en *tokens* de las tradicionales cuentas de reservas y liquidación. La utilidad real de las CBDC mayoristas basadas en DLT depende del potencial de esta tecnología para mejorar la eficiencia y reducir los costes operacionales y de liquidación. Los beneficios podrían ser sustanciales, dado que muchos de los actuales sistemas de pagos mayoristas operados por bancos centrales se basan en tecnologías anticuadas y caras de mantener.

Dos son los principales retos para la implantación de estas CBDC mayoristas. El primero, que las limitaciones de la DLT sin permisos también afectan a las CBDC, por lo que estas últimas deben basarse en protocolos con permisos. El segundo, que las opciones de diseño para la convertibilidad entre las reservas en el banco central y la moneda digital en el registro distribuido deben aplicarse con cautela, a fin de mantener la liquidez intradía y minimizar al mismo tiempo los riesgos de liquidación.

Varios bancos centrales, entre los que cabe citar al Banco de Canadá (proyecto Jasper), el BCE, el Banco de Japón (proyecto Stella) y la Autoridad Monetaria de Singapur (proyecto Ubin), ya han experimentado con sistemas RTGS mayoristas para CBDC basadas en DLT. En la mayoría de los casos, los bancos han optado por un enfoque basado en un certificado de depósito digital (DDR), por medio del cual el banco central emite *tokens* digitales con asiento en un registro distribuido que están respaldados y pueden ser reembolsados por reservas en el banco central mantenidas en una cuenta segregada. Los *tokens* pueden utilizarse para realizar transferencias interbancarias en un registro distribuido.

Actualmente los bancos centrales están publicando sus resultados. En sus fases iniciales, todos los experimentos lograron replicar con considerable éxito los actuales sistemas de pagos de elevada cuantía. Sin embargo, los resultados de estos *tokens* no han sido claramente superiores a los de las actuales infraestructuras①.

① Véase M. Bech y R. Garratt, «Criptomonedas de bancos centrales», *Informe Trimestral del BPI*, septiembre de 2017, y Comité de Pagos e Infraestructuras del Mercado y Comité de los Mercados, *Monedas digitales emitidas por bancos centrales*, marzo de 2018.

Notas

[1] La terminología sobre este tema es inestable y continúa evolucionando, con las consiguientes ambigüedades jurídicas y reguladoras. El uso del término «criptomonedas» en este capítulo no pretende expresar ninguna opinión sobre la naturaleza de los sistemas subyacentes basados en protocolos. Por lo general, las criptomonedas tienen algunas de las características (pero no todas) de una moneda soberana y su consideración jurídica varía de unas jurisdicciones a otras. En determinados casos, el capítulo cita como ejemplos criptomonedas o criptoactivos concretos. Estos ejemplos no son exhaustivos y no deben interpretarse como la aprobación por parte del BPI o de sus accionistas de una determinada criptomoneda, empresa, producto o servicio.

[2] Sobre esta cuestión, véanse también Carstens (2018a,c).

[3] Graeber (2011) afirma que el dinero no se generalizó hasta que se inventó la moneda, que surgió de forma casi simultánea en China, la India y Lidia entre los años 600 y 500 a.C. aproximadamente. También explica que, al contrario de lo que se suele creer, antes de que se utilizara el dinero los intercambios se llevaban a cabo mayoritariamente mediante pagarés al portador, y no mediante trueque.

[4] Estas funciones del dinero se han estudiado ampliamente en la literatura. A continuación se citan algunos ejemplos. Kiyotaki y Wright (1989) muestra que el dinero, utilizado como medio de pago, puede mejorar los resultados del trueque. Kocherlakota (1996) sostiene que cuando no son posibles un registro perfecto y el compromiso, el dinero mejora los resultados al servir de «memoria». Samuelson (1958) demuestra en un modelo de generaciones solapadas que el dinero puede mejorar la eficiencia cuando se usa como depósito de valor. Doepke y Schneider (2017) presenta la mejora de resultados que se obtiene utilizando una unidad de cuenta común y explica por qué el dinero público es una unidad de cuenta y un medio de cambio al mismo tiempo.

[5] Ejemplos de objetos utilizados como dinero mercancía incluyen conchas marinas en África, granos de cacao en la civilización azteca y *wampum* (cinturones de abalorios) en las colonias de América del Norte. Incluso en estos casos, no cabe duda de que estos mecanismos coexistieron con relaciones de crédito. Véase, por ejemplo, Melitz (1974) para un análisis más detallado.

[6] Sobre la evolución de las cartas de crédito y la función esencial que han desempeñado en el desarrollo de los sistemas monetarios en general y en la financiación del comercio en particular, véase De Roover (1948, 1953). Para un análisis exhaustivo y una descripción histórica, véase Kindleberger (1984), que aborda el tema en general, y Santarosa (2015), que se centra en la importancia de la introducción de la responsabilidad solidaria.

[7] El dinero público respaldado por mercancías de valor intrínseco, como el patrón oro, fue otro intento de lograr un equilibrio. Pese a aportar estabilidad en periodos normales, sus restricciones han tendido a limitar la capacidad de los bancos centrales para suministrar dinero de forma elástica en épocas de tensiones financieras y económicas. A menudo, en circunstancias extremas estas restricciones simplemente se han obviado, optándose por la inconvertibilidad. Por ejemplo, bajo el patrón oro, la obligación de convertibilidad en oro se podía considerar una restricción de la capacidad del Estado para devaluar la moneda mediante su sobreemisión. Esta restricción resultaba creíble precisamente porque las mercancías tienen valor de mercado en su uso no monetario, es decir, cuando no se usan como medio de pago sino con otros fines. Esto impedía que los Estados sometieran a los tenedores a su poder monopolístico. Véase una discusión más amplia en Giannini (2011).

[8] Para un estudio más reciente, incluido un análisis de los incentivos para devaluar la moneda, véase Schnabel y Shin (2018).

[9] Véanse Van Dillen (1964), Roberds y Velde (2014) y Bindseil (2018). Para saber más sobre la relación con la banca central, véanse Ugolini (2017), Bindseil (2018) y Schnabel y Shin (2018).

[10] Además, los bancos centrales han gozado normalmente de la flexibilidad necesaria para actuar como prestamistas de última instancia. La reciente Gran Crisis Financiera fue un nuevo recordatorio tanto de la fragilidad como de la capacidad de adaptación de los actuales sistemas monetarios, incluso en las economías más avanzadas. Aunque la crisis reveló las deficiencias del marco regulador vigente, la creciente atención prestada a la regulación y la supervisión bancarias una vez superada pone de manifiesto la capacidad de los mecanismos institucionales para evolucionar con el fin de mantener la confianza en el dinero en el marco general del sistema de dos niveles.

[11] Véase Carstens (2018a). Giannini (2011) también subraya la importancia de los mecanismos institucionales a través de los cuales se suministra el dinero: «La evolución de las instituciones monetarias parece ser, sobre todo, fruto de un diálogo continuo entre las esferas económica y

política, que se turnan para crear innovaciones financieras [...], así como para proteger el interés común ante los abusos derivados de intereses partidistas».

[12] Así, actualmente los bancos centrales vigilan los sistemas de pago y proporcionan grandes volúmenes de crédito intradía para lograr precisamente este resultado, sobre todo en sistemas de pagos mayoristas. Dependiendo de las características específicas de los mecanismos, también pueden conceder este crédito a un día o con vencimientos más largos. Para una descripción más exhaustiva de los mecanismos, los procedimientos operacionales y otras cuestiones, véase BPI (1994) y Borio (1997).

[13] Véanse Bech y Garratt (2017) y CPMI-MC (2018) para un análisis detallado.

[14] Como ocurre también en gran medida en el caso de los billetes bancarios y otros *tokens* físicos, cada transacción se verifica por referencia al objeto de pago: la respectiva inscripción en el registro. Aquí radica la diferencia con otras formas de dinero electrónico, cuya verificación se basa en la identidad del titular de la cuenta. Por lo tanto, las criptomonedas son dinero digital basado en *tokens*.

[15] Entre los ejemplos actuales o previstos de criptomonedas que utilizan un modelo con permisos y nodos de confianza designados se incluyen la moneda que emitirá la SAGA Foundation, Ripple y Utility Settlement Coin.

[16] Utilizamos el término «Bitcoin» para hacer referencia al protocolo y la red de usuarios y mineros de la criptomoneda y «bitcoin» para aludir a la unidad de la moneda.

[17] Entre los ejemplos cabe citar Ethereum, Litecoin y Namecoin.

[18] Auer (2018) presenta una descripción detallada de los elementos tecnológicos del Bitcoin y otras criptomonedas basadas en la cadena de bloques, como las firmas digitales, el *hashing* y la unión criptográfica de los bloques. Véase también Berentsen y Schär (2018).

[19] Técnicamente, esto se lleva a cabo por medio de funciones criptográficas denominadas «*hash*» (SHA-256 en el caso del Bitcoin). Estas funciones se caracterizan por la imposibilidad de predecir los resultados, por lo que la única forma de generar un resultado concreto es mediante prueba y error.

[20] Para que una criptomoneda sin permisos funcione en un entorno en el que no existe ninguna autoridad central generadora de confianza, todos los mineros y usuarios deben almacenar una copia actualizada del registro íntegro. Sin embargo, en la práctica muchos usuarios confían en la información facilitada por otros. Algunos solo comprueban el resumen del registro por medio de un proceso denominado verificación simplificada de pago. Además, contraviniendo el precepto original del Bitcoin, un número aún mayor de usuarios solo puede acceder a sus fondos a través del sitio web de un tercero. En estos casos, ese tercero controla en solitario las posiciones en criptomonedas de sus clientes.

[21] Nakamoto (2009), p. 8.

[22] Esto se logra mediante la calibración automática de la prueba de trabajo, que incrementa la dificultad matemática hasta que la potencia computacional de todos los mineros sumada baste para actualizar el registro a la velocidad prefijada por el protocolo.

[23] Véase Carstens (2018a).

[24] Aunque la congestión podría resolverse permitiendo la existencia de bloques mayores, esto podría resultar aún más destructivo. Sin tener en cuenta la retribución por cada bloque, cierto nivel de congestión es esencial para instar a los usuarios a pagar por las transacciones, puesto que si el sistema funcionara por debajo de su límite, todas las transacciones se procesarían y un usuario racional pagaría comisiones casi nulas. En ese caso, los mineros no obtendrían ninguna ventaja por actualizar las transacciones y el equilibrio podría romperse. Véanse, en particular, Hubermann et al (2017) y Easley et al (2017), así como Abadi y Brunnermeier (2018).

[25] Técnicamente hablando, la relación entre los usuarios es de sustitutos estratégicos, no de complementos estratégicos. Por lo tanto, las criptomonedas son más un juego de congestión que un juego de coordinación.

[26] El carácter probabilístico de la firmeza podría generar riesgos agregados si las criptomonedas se utilizaran en contextos mayoristas, en los que los fondos suelen reinvertirse de forma inmediata. De hecho, esto generaría una dimensión completamente nueva de riesgo agregado, ya que las exposiciones estarían relacionadas entre sí por la probabilidad de que todo el historial de transacciones no pueda considerarse firme.

[27] Las soluciones propuestas no son pocas, pero la mayoría todavía no se han llevado a la práctica. Por una parte, es posible que los futuros protocolos de criptomonedas acaben con las costosas pruebas de trabajo, sustituyéndolas con «pruebas de participación» que consisten en lograr credibilidad

mediante la acumulación de posiciones en criptomonedas, en lugar de mediante un oneroso trabajo informático. Las soluciones propuestas para la falta de escalabilidad incluyen Lightning Network, una red que básicamente saca pequeñas transacciones (micropagos) de la cadena de bloques principal para trasladarlas a un entorno prefinanciado independiente. También hay nuevas criptomonedas, como la IOTA, que pretenden reemplazar la cadena de bloques con una estructura de registro y verificación más compleja.

[28] Véase Juskalian (2018).

[29] Véanse Carstens (2018a,b).

[30] Tampoco los funcionarios públicos son inmunes al atractivo de las criptomonedas: dos agentes del Gobierno estadounidense han sido acusados de la sustracción de bitcoins confiscados durante el cierre de Silk Road.

[31] Por ejemplo, la mayoría de los pagos en bitcoins a través de un *smartphone* se realizan muy probablemente a través de un tercero, dado que el tamaño actual de la cadena de bloques supera la capacidad de almacenamiento de la mayoría de esos teléfonos. Reuters (2017) y Moore y Christin (2013) citan casos en los que esos terceros han resultado ser entidades implicadas en actividades fraudulentas o han sufrido ataques informáticos. Para un análisis de los usos ilícitos de las criptomonedas, véase Fanusie y Robinson (2018) y Foley et al (2018).

[32] Véase Ministros de Finanzas y Gobernadores de Bancos Centrales del G-20 (2018).

[33] Comparando la regulación de las OIC con la de las OPI en el contexto estadounidense, Clayton (2017) sostiene que «una alteración de la estructura de una oferta de valores no cambia lo fundamental: cuando se ofrece un valor, deben cumplirse nuestra legislación en materia de valores». FINMA (2018) establece un marco regulador en Suiza que clasifica las OIC en función de la utilización que se prevé para los *tokens* emitidos: como pagos, activos o *utility tokens*.

[34] Técnicamente, para que una criptomoneda basada en protocolos comience a operar basta con que un solo país autorice el acceso. Las dificultades que las autoridades han tenido para cerrar sitios de descargas ilegales como Napster o The Pirate Bay y protocolos de descarga como BitTorrent evidencian los problemas que existen para garantizar el cumplimiento de la normativa.

[35] El Grupo de Acción Financiera (2015) sostiene que el tratamiento uniforme entre jurisdicciones de productos y servicios similares, con arreglo a su función y su perfil de riesgo, es esencial para incrementar la eficacia de las normas internacionales para luchar contra el blanqueo de capitales.

[36] Una complicación es que los pagos están regulados por autoridades y legislaciones con objetivos muy distintos, como la vigilancia del sistema de pagos, la supervisión prudencial, la protección de los consumidores, la prevención de la financiación del terrorismo y la lucha contra el blanqueo de capitales. Por ejemplo, las instituciones domiciliadas en Estados Unidos han de cumplir, entre otras, la ley del secreto bancario (Bank Secrecy Act), la ley antiterrorista bautizada como USA PATRIOT Act y la normativa de control de activos extranjeros de la Office of Foreign Assets Control. Otra dificultad está relacionada con la aplicabilidad de la actual legislación a los nuevos instrumentos. Por ejemplo, la definición de dinero electrónico en la Unión Europea exige que los saldos representen un activo frente al emisor. Al no cumplir este precepto, las criptomonedas no pueden considerarse dinero electrónico y, por defecto, no están sujetas a la legislación correspondiente.

[37] Las CBDC basadas en *tokens* podrían implementarse desde el punto de vista técnico de muy diversas formas. Podrían estar basadas en DLT y compartir características con las criptomonedas, con la salvedad de que sería el banco central, y no el propio protocolo, el que controlaría el importe emitido y garantizaría el valor del *token*.

[38] CPMI-MC (2018).

Referencias bibliográficas

Abadi, J. y M. Brunnermeier (2018): «Blockchain economics», Princeton University, mimeo, mayo.

Auer, R. (2018): «The mechanics of decentralised trust in Bitcoin and the blockchain» *BIS Working Papers*, próxima publicación.

Banco de Pagos Internacionales (1994): *64ºInforme Anual,* junio.

Bech, M. y R. Garratt (2017): «Criptomonedas de bancos centrales», *Informe Trimestral del BPI*, septiembre de 2017.

Berentsen, A. y F. Schär (2018): «A short introduction to the world of cryptocurrencies», Federal Reserve Bank of St Louis, *Review*, vol. 100, nº 1.

Bindseil, U. (2018): «Pre-1800 central bank operations and the origins of central banking», Mannheim University, mimeo.

Borio, C. (1997): «The implementation of monetary policy in industrial countries: a survey», *BIS Economic Papers* nº 47, julio.

Carstens, A. (2018a): «Money in the digital age: what role for central banks?», discurso pronunciado en House of Finance, Goethe University, Fráncfort, 6 de febrero.

Carstens, A. (2018b): «Central banks and cryptocurrencies: guarding trust in a digital age», intervención en Brookings Institution, Washington DC, 17 de abril.

Carstens, A. (2018c): «Technology is no substitute for trust», *Börsen-Zeitung*, 23 de mayo.

Catalini, C., J. Boslego y K. Zhang (2018): «Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings», *MIT Working Papers*, próxima publicación.

Clayton, J. (2017): «Statement on cryptocurrencies and initial coin offerings», www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 11 de diciembre.

Comité de Pagos e Infraestructuras del Mercado (CPMI) y Comité de los Mercados (2018): *Monedas digitales emitidas por bancos centrales*, marzo.

De Roover, R. (1948): *Money, banking and credit in mediaeval Bruges: Italian merchant-bankers, Lombards and money changers - a study in the origins of banking*, Mediaeval Academy of America.

De Roover, R. (1953): *L'évolution de la letter de change: XIVe-XVIIIe siècle*, Armand Colin.

Doepke, M. y M. Schneider (2017): «Money as a unit of account», *Econometrica*, vol. 85, nº 5, pp. 1537-74.

Easley, D., M. O'Hara y S. Basu (2017): «From mining to markets: The evolution of Bitcoin transaction fees», papers.ssrn.com/sol3/papers.cfm?abstract_id=3055380.

Fanusie, Y. y T. Robinson (2018): «Bitcoin laundering: an analysis of illicit flows into digital currency services», C*enter on Sanctions & Illicit Finance memorandum*, enero.

Financial Market Supervisory Authority (FINMA) (2018): *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16 de febrero.

Foley, S., J. Karlsen y T. Putniņš (2018): «Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?», dx.doi.org/10.2139/ssrn.3102645.

Giannini, C. (2011): *The age of central banks*, Edward Elgar.

Graeber, D. (2011): *Debt: the first 5,000 years*, Melville House.

Grupo de Acción Financiera (2015): *Guidance for a risk-based approach to virtual currencies*, junio.

Huberman, G., J. Leshno y C. Moellemi (2017): «Monopoly without a monopolist: an economic analysis of the Bitcoin payment system», *Columbia Business School Research Papers*, nº 17-92.

Juskalian, R. (2018): «Inside the Jordan refugee camp that runs on blockchain», *MIT Technology Review*, edición en línea, 12 de abril.

Kindleberger, C. (1984): *A financial history of western Europe*, Allen & Unwin.

Kiyotaki, N. y R. Wright (1989): «On money as a medium of exchange», *Journal of Political Economy*, vol. 97, nº 4, pp. 927-54.

Kocherlakota, N. (1996): "Money is memory", *Journal of Economic Theory*, vol. 81, issue 2, pp. 232–51.

Melitz, J. (1974): *Primitive and modern money: an interdisciplinary approach*, Addison-Wesley.

Ministros de Finanzas y Gobernadores de Bancos Centrales del G-20 (2018): Comunicado de la Cumbre de Buenos Aires, 19 y 20 de marzo.

Moore, T. y N. Christin (2013): «Beware the middleman: empirical analysis of Bitcoin-exchange risk», en A-R. Sadeghi (ed.), *Lecture Notes in Computer Science*, vol. 7859.

Nakamoto, S. (2009): «Bitcoin: a peer-to-peer electronic cash system», white paper.

Reuters (2017): «Cryptocurrency exchanges are increasingly roiled by hackings and chaos», 29 de septiembre.

Roberds, W. y F. Velde (2014): «Early public banks», *Federal Reserve Bank of Chicago Working Papers*, nº 2014-03.

Samuelson, P. (1958): «An exact consumption-loan model of interest with or without the social contrivance of money», *Journal of Political Economy*, vol. 66, nº 6, pp. 467-82.

Santarosa, V. (2015): «Financing long-distance trade: the joint liability rule and bills of exchange in eighteenth-century France», *The Journal of Economic History*, vol. 75, nº 3, pp. 690–719.

Schnabel, I. y H. S. Shin (2018): «Money and trust: lessons from the 1620s for money in the digital age», *BIS Working Papers*, nº 698, febrero.

Ugolini, S. (2017): *The evolution of central banking: theory and history*, Palgrave-Macmillan.

Van Dillen, J. G. (1964): *History of the principal public banks*, Frank Cass & Co.