TEMA DE ANÁLISIS / N°15

¿TIENEN LAS CRIPTOMONEDAS LOS ATRIBUTOS NECESARIOS PARA REEMPLAZAR AL DINERO ACTUAL? POSICIÓN DEL BANCO DE PAGOS INTERNACIONALES (BIS) - REPORTE ECONÓMICO ANUAL - JUNIO 2018

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

AGOSTO | 2018

La historia nos ha enseñado que la esencia de un buen dinero ha sido siempre la confianza en la estabilidad de su valor y el acuerdo social e institucional a través del cual el dinero es emitido. En otras palabras, el dinero debe tener 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 hacer esto posible, actualmente se requieren determinados mecanismos institucionales, y por ello, surgen los bancos centrales, con su autonomía y su obligación de rendir cuentas.

Debido a la importancia del dinero y, por ende, de sus potenciales sustitutos, el Banco de Pagos Internacionales (BIS por su sigla en inglés), abordó en su reporte económico anual, la interrogante sobre si realmente las criptomonedas pueden cumplir el rol de dinero y, si no es así, qué problemas económicos específicos podrían realmente resolver [1]. A continuación, resumiremos esta sección del reporte del BIS, no sin antes dar una pequeña explicación sobre qué es el BIS y cuál es su labor.

El BIS es una organización internacional financiera propiedad de numerosos bancos centrales. Conocido como el "banco de los bancos centrales", el BIS fomenta la cooperación financiera y monetaria internacional y sirve de banco para los bancos centrales. Esta organización no rinde cuentas ante ningún gobierno y lleva a cabo su trabajo a través de sus departamentos monetario, económico y bancario, su secretaría general y a través de su Asamblea General, en la que tienen derecho de voto y representación sus bancos centrales miembros. Además, presta servicios bancarios a bancos centrales y otras instituciones monetarias oficiales.

A casi 10 años de su creación, las criptomonedas han logrado captar la atención del mundo con la promesa de reemplazar la confianza en instituciones como los bancos privados y los bancos centrales, por confianza en un sistema completamente descentralizado soportado por blockchain y tecnología de registro contable distribuido (DLT).

Sin embargo, la creación descentralizada de la confianza tiene limitaciones económicas inherentes. Para que se mantenga la confianza, es necesario que: los participantes honestos de una red controlen la gran mayoría del poder computacional; que todos y cada uno de los usuarios verifiquen la historia de las transacciones; y que la emisión de la criptomoneda esté predeterminada por su protocolo.

[1] Es necesario advertir que, debido a que el BIS es una organización propiedad de los bancos centrales, y las criptomonedas son una potencial futura competencia al monopolio de la emisión de dinero, podría estar existiendo un cierto grado de conflicto de interés en la postura de esta organización. Aun así, consideramos de gran interés conocer la posición de esta organización, y sus respectivos fundamentos, sobre las criptomonedas y su tecnología.

Además, esta creación descentralizada de confianza implica ciertos riesgos. Ésta podría diluirse en cualquier momento debido a la fragilidad del consenso descentralizado a través del cual se registran las transacciones, ya que la criptomoneda podría simplemente dejar de funcionar, lo que daría como resultado una pérdida total de valor.

Incluso si se pudiese mantener la confianza, la tecnología de criptomonedas, hasta el momento, ha mostrado ser poco eficiente y demanda un gran uso de energía. Las criptomonedas no pueden adaptar su oferta a la demanda de transacciones, son propensas a la congestión y fluctúan enormemente de valor. Por lo anterior, en general, la tecnología descentralizada de las criptomonedas, por muy sofisticada que sea, es, por el momento, un mal sustituto del dinero y su respaldo institucional, debido al riesgo de fraude, a la gran volatilidad de su valor y al enorme costo medioambiental y energético[2]. De hecho, para los más escépticos, las criptomonedas son "una combinación de burbuja, juego de Ponzi y desastre ambiental".

Sin embargo, la tecnología subyacente a las criptomonedas denominada blockchain o cadena de bloques podría ser prometedora en otras aplicaciones, como la simplificación de los procesos administrativos en la liquidación de actas, procesos de auditoría, registros contables o elaboración de contratos inteligentes. Por esto, es importante regular los usos públicos y privados de esta tecnología, discutir las medidas necesarias para prevenir el fraude y evaluar la posible emisión de monedas digitales por parte de los bancos centrales.

Rol del dinero y funcionamiento de los actuales sistemas monetario y de pagos

El dinero juega un rol fundamental en facilitar el intercambio económico desde que las sociedades se hicieron las complejas y la actividad económica se expandió. Éste tiene 3 roles fundamentales y complementarios:

1. Unidad de cuenta: permite simplificar la comparación de precios relativos entre los bienes.
2. Medio de intercambio: a partir de un acuerdo social, un vendedor lo acepta como medio de pago a cambio de que en el futuro se lo acepten a él como medio de pago.
3. Reserva de valor: permite transferir poder de compra a través del tiempo.

[2] Algunos expertos en informática sostienen que el problema del costo medioambiental y energético tendrías una solución factible con el uso de la computación cuántica.

Actualmente existe consenso en que la forma apropiada de proveer confianza en una moneda es a través de un banco central independiente, ya que permite tener:

1. Objetivos claros de política monetaria y estabilidad financiera.
2. Independencia operativa, administrativa y en la elección de instrumentos de política.
3. *Accountability* democrática, o rendición de cuentas democrática, que permite obtener legitimidad en el plano político.

En la actualidad, 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.

De hecho, el banco central toma un rol activo en la supervisión y, en algunos casos, en la provisión y vigilancia de la infraestructura de pagos para su moneda. Así también, debe garantizar que el sistema de pagos funcione sin problemas y asegurarse de que el suministro de reservas responda adecuadamente a la demanda cambiante, incluso a la frecuencia intradía, es decir, garantizando una oferta monetaria lo suficientemente elástica.

Por lo anterior, gracias a la figura de un banco central que respalda la confianza en la moneda, los sistemas de pago hoy en día son seguros y eficientes en costos, y además se caracterizan por su escalabilidad y la autenticidad de los pagos una vez realizados[3].

Un atributo operacional deseable en los sistemas de pago es la certeza del pago (o finalidad del pago, que se refiere a la autenticidad de éste y su carácter definitivo), así como la capacidad de impugnar transacciones que pueden haberse ejecutado incorrectamente. Esta finalidad requiere que el sistema esté libre de fraude y riesgos operacionales, tanto a nivel de transacciones individuales como del sistema en su conjunto.

Así, se distinguen cuatro propiedades clave del dinero: el emisor, la forma, el grado de accesibilidad y el mecanismo de transferencia de pago. El emisor puede ser un banco central, un banco privado o comercial, o incluso nadie, como cuando el dinero tomaba la forma de una mercancía. Su forma puede ser física, por ejemplo, una moneda metálica o un billete de papel, o digital. Puede ser ampliamente accesible, al igual que los depósitos de bancos comerciales, o de manera restringida, como las reservas del banco central. La última propiedad se refiere al mecanismo de transferencia, que puede ser de igual a igual

[3] Al ser los sistemas de pago seguros y eficientes, permiten gestionar grandes volúmenes y adaptarse al rápido incremento de los pagos a costos reducidos. Un factor determinante para la seguridad y la eficiencia es la escalabilidad del sistema actual. En éste, el creciente uso del instrumento de pago no se traduce en un incremento proporcional de los costos. Esta característica es de suma relevancia, 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, ya que mientras más usuarios se conectan a un sistema de pago, más incentivos tienen para utilizarlo quienes todavía no participan en él.

(directamente entre las partes o *peer-to-peer*), o a través de un intermediario central, como en el caso de los depósitos.
El dinero generalmente se basa en una de las dos tecnologías básicas: los denominados *tokens* (vales o fichas) o cuentas. El dinero basado en *tokens*, por ejemplo, billetes de banco o monedas físicas, puede intercambiarse directamente entre las partes, pero dicho intercambio depende críticamente de la capacidad del beneficiario de verificar la validez del objeto utilizado para el pago (en el caso del efectivo, la preocupación es la falsificación). Por el contrario, los sistemas basados en el dinero de la cuenta dependen fundamentalmente de la capacidad de verificar la identidad del titular de la cuenta.

Criptomonedas y la promesa de confianza descentralizada

La promesa de las criptomonedas consiste en ser una nueva forma de moneda y mantener la confianza y la estabilidad de su valor a través del uso de la tecnología.

Las criptomonedas se basan en tres elementos fundamentales. Primero, en un conjunto de reglas -el protocolo-, que consiste en un código computacional que especifica cómo los participantes pueden realizar las transacciones. En segundo lugar, un libro contable mayor que almacena el historial de todas las transacciones realizadas. Y tercero, una red descentralizada de participantes que comprueban el registro de las transacciones y actualizan, almacenan y leen el libro contable mayor de las transacciones siguiendo las reglas del protocolo.

Aunque se crean de manera privada, las criptomonedas no son responsabilidad de nadie, es decir, no pueden ser canjeadas, y su valor se deriva únicamente de la expectativa de que continuarán siendo utilizadas y aceptadas por otros. Esto las hace parecidas a un dinero mercancía (aunque sin ningún valor intrínseco en uso) que permite el intercambio digital entre pares (*peer-to-peer*).

En comparación con otros dineros digitales privados, como los depósitos bancarios, la característica distintiva de las criptomonedas es el intercambio digital entre pares. A diferencia de las cuentas bancarias digitales o las “monedas virtuales” emitidas por privados, las transferencias de criptomonedas pueden tener lugar, en principio, en un entorno descentralizado sin la necesidad de una contraparte central para ejecutar el intercambio.

Tecnología de contabilidad distribuida en criptomonedas

El desafío tecnológico en el intercambio digital entre pares (*peer-to-peer*) es el denominado "problema de doble gasto": cualquier forma de dinero digital es fácilmente replicable y, por lo tanto, se puede gastar fraudulentamente más de una vez, de hecho, es más fácil reproducir información digital que falsificar billetes bancarios. Por lo tanto, para poder usar dinero digital, se debe resolver este problema, lo que requiere, como mínimo, que alguien mantenga un registro de todas las transacciones.

Antes de la irrupción de las criptomonedas, la única solución a este problema era hacer que un agente centralizado verificara todas las transacciones. Luego, las criptomonedas superaron el problema del doble gasto a través de un registro descentralizado a través de lo que se conoce como un libro mayor distribuido. El libro mayor se puede considerar como un archivo o registro que comienza con una distribución inicial de criptomonedas y registra el historial de todas las transacciones posteriores y cambios de propiedad de las criptomonedas.

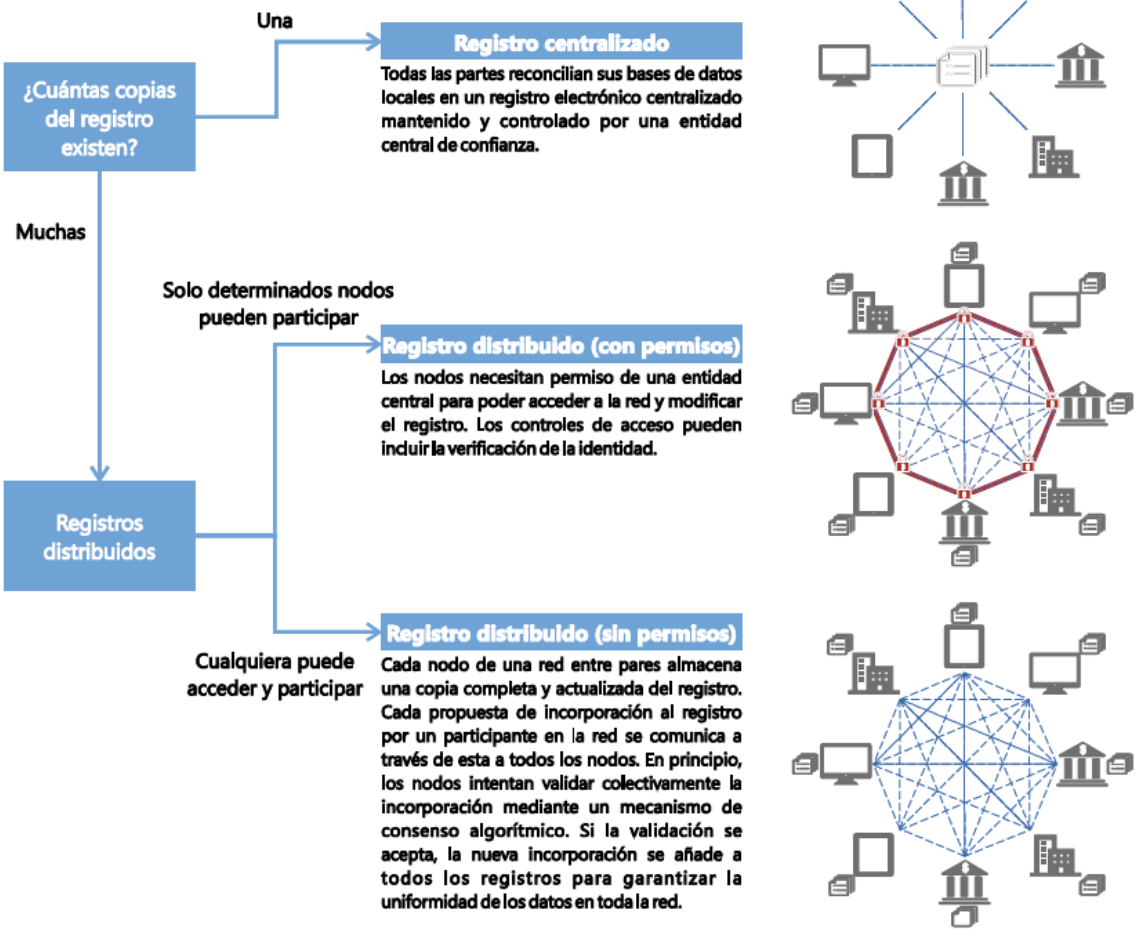
Cada usuario de la red almacena una copia actualizada de todo el libro (esto es lo que lo hace "distribuido"). Con un libro mayor distribuido, el intercambio de dinero digital entre pares es factible, ya que cada usuario puede verificar directamente en su copia del libro contable si se realizó una transferencia y si no hubo intento de realizar un doble gasto.
Si bien todas las criptomonedas dependen de un libro mayor distribuido, difieren en términos de cómo se actualiza el libro mayor. Así, es posible distinguir dos tipos de criptomonedas en base a las diferencias en su configuración operativa (ver Figura 1):

- Las criptomonedas del primer tipo son similares a los mecanismos de pago convencionales en que, para evitar fraudes, el libro mayor solo puede ser actualizado por participantes autorizados, a menudo denominados "nodos de confianza". Estos nodos son elegidos por (y están sujetos a la supervisión de) una autoridad central, por ejemplo, la empresa que desarrolló la criptomoneda. Por lo tanto, mientras que las criptomonedas basadas en sistemas autorizados difieren del dinero convencional en términos de cómo se almacenan los registros de transacciones (descentralizados versus centralizados), comparten con él la dependencia de instituciones específicas como la fuente principal de confianza.

- El segundo tipo de criptomonedas se componen por una desviación mucho más radical de la configuración predominante basada en instituciones. Éstas prometen generar confianza en un entorno completamente descentralizado. Las transacciones de registro del libro mayor solo se pueden cambiar por consenso de los participantes en la moneda: mientras que cualquier persona puede participar, nadie tiene una clave especial para cambiar el libro mayor.

Dentro de este segundo grupo de criptomonedas, la primera que surge es el Bitcoin y el libro de contabilidad distribuido denominado *blockchain* o cadena de bloques. Éste se actualiza en grupos de transacciones llamadas bloques. Los bloques se encadenan secuencialmente a través del uso de la criptografía para formar la cadena de bloques. A partir de 2009, esta tecnología se ha adaptado a innumerables otras criptomonedas.

Figura 2: Registro centralizado y registro descentralizado con y sin permisos

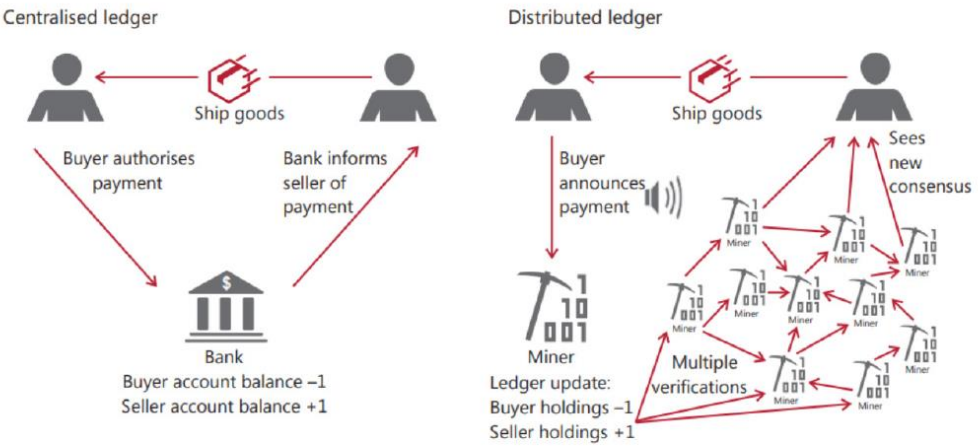


		Dinero electrónico privado basado en un sistema fiduciario	Criptomonedas de emisores privados	
			Con permisos	Sin permisos
1	Almacenamiento de saldos/posiciones	Registro (cuentas) almacenado de forma centralizada por bancos y otras instituciones financieras	Almacenamiento descentralizado del registro	
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	Procedimiento 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 fimeza/ 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 intradia	El protocolo puede ser modificado por nodos de confianza	Fijada por el protocolo
6	Mecanismos de generación de confianza	Reputacion de bancos y bancos centrales, supervisión bancaria, prestamista de última instancia, legislación sobre moneda de curso legal, independencia y obligación de rendr 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

Fuente: Traducido de Natarajan et al. (2017), "Distributed Ledger Technology (DLT) and Blockchain", Grupo del Banco Mundial, FinTech Note, nº 1; BPI.

Las criptomonedas basadas en *blockchain* tienen dos grupos de participantes: los "mineros", que actúan como validadores de las transacciones; y los "usuarios", que quieren realizar transacciones de la criptomoneda. En términos generales, la idea subyacente de estas criptomonedas es simple: en lugar de que un banco centralmente registre las transacciones, el libro mayor es actualizado por un minero y todos los usuarios y mineros almacenan la actualización (ver Figura 3).

Figura 3: Validación de transacciones en un registro centralizado/cuenta bancaria y en una criptomoneda descentralizada



Un comprador compra un bien a un 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, 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 descentralizada, el comprador primero anuncia públicamente una orden de pago, con la cual la cantidad de la criptomoneda que posee el comprador se reduce, mientras que la del vendedor se incrementa. Luego, 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: Traducido de Auer, "The Mechanics of Decentralised Trust in Bitcoin and the Blockchain", BIS Working Papers.

La característica fundamental de estas criptomonedas, que sustenta el sistema, es la aplicación de un conjunto de normas (el "protocolo"), que alinea los incentivos de todos los participantes y crea así una tecnología de pago confiable sin la necesidad de contar con un agente de confianza central. Además, a partir del protocolo, todos los participantes cumplen las normas por su propio interés, es decir, se genera un equilibrio autosostenible. Los tres aspectos fundamentales en este ámbito son:

- En primer lugar, el protocolo hace que la actualización del registro tenga un costo. En la mayoría de los casos, este costo se debe a que, para poder introducir modificaciones en el registro, se exige una "prueba de trabajo[4]", que consiste en 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 energético no menor. Este proceso se denomina minería, y 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 incorporar 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 incentivarlos a añadir a la cadena únicamente transacciones válidas.

- 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 o actualizaciones que incluyen distintos conjuntos de operaciones.

A partir de lo anterior, 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

[4] Para más detalles, puedes ver nuestro Estudio sobre Bitcoin y Tecnología Blockchain, disponible en: https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514112818/estudio_sobre_bitcoin_y__tecnolog__a_blockchain.pdf

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 produjo en forma paralela. Por consiguiente, para que un ataque de doble gasto (o fraude) tenga éxito, se requiere controlar un porcentaje significativo de la potencia computacional de la red minera, lo que es muy poco probable dado el actual tamaño de la red en el caso de Bitcoin, pero es un riesgo latente en el caso de las criptomonedas recientemente creadas.

Análisis de las limitaciones económicas de las criptomonedas descentralizadas

De acuerdo con lo afirmado en este estudio, el funcionamiento de una criptomoneda requiere que se cumplan varias condiciones, entre éstas, 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.

Ahora cabe analizar si el proceso a través del cual esta tecnología genera confianza es eficiente y si la confianza generada está garantizada ante cualquier circunstancia.

Con respecto a la eficiencia del proceso, es posible que el enorme costo de generar confianza de forma descentralizada se transforme prontamente en una limitación. Las instalaciones que utilizan los mineros pueden llegar a albergar la potencia computacional equivalente a la de millones de ordenadores personales. A modo de ejemplo, en la actualidad, el consumo total de electricidad de la red de Bitcoin equivale al de economías medianas como Suiza.

Sin embargo, los problemas económicos subyacentes van mucho más allá del consumo de energía, y están relacionados con una de las características más importantes del dinero que es la capacidad de promover externalidades de red entre los usuarios y servir así como mecanismo de coordinación de la actividad económica.

En este aspecto, las criptomonedas presentan deficiencias en tres dimensiones: escalabilidad, estabilidad del valor y confianza en el carácter definitivo de los pagos.

En primer lugar, las criptomonedas no pueden aumentar su escala de forma sencilla como sucede con el dinero tradicional. 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 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 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 se vuelve estrictamente limitada.

Para procesar el número de transacciones digitales minoristas que se tramitan actualmente a través de una selección de sistemas nacionales de pagos minoristas, el tamaño del registro superaría ampliamente la capacidad de un computador normal y la de un servidor tradicional. Pero el problema no se circunscribe a la capacidad de almacenamiento, sino que afecta también a la de procesamiento: solo los supercomputadores 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[5].

Otro aspecto del problema de escalabilidad es que la actualización del registro puede congestionarse. 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 mismo tiempo, las comisiones se disparan cada vez que la demanda de transacciones alcanza dicho límite. Esto limita la utilidad de las criptomonedas para las transacciones cotidianas y/o diarias.

Por lo anterior, mientras más gente utiliza una criptomoneda, más laboriosos son los pagos. Se incumple así una propiedad esencial del dinero que hoy en día necesitamos, que es que mientras más personas lo utilizan, mayor es el incentivo para usarlo.

El segundo problema fundamental de las criptomonedas es la gran volatilidad de su valor, debida a la ausencia de un emisor centralizado al que se haya encomendado el objetivo de estabilidad monetaria. 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. 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, produciendo su alta volatilidad. Si bien se han diseñado monedas que intentan mantener paridad con alguna moneda como el dólar, éstas no han sido exitosas. La razón es que mantener una oferta de medios de pago ajustada a la demanda de transacciones obliga a tener una autoridad 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 los incentivos para estabilizar el valor de la moneda: si la demanda de la criptomoneda se reduce, su precio también baja.

A lo anterior se suma la acelerada creación de nuevas criptomonedas. Si revisamos las experiencias de la banca privada en el pasado, la acelerada creación y emisión de nuevas formas de dinero rara vez genera estabilidad.

[5] Equivalente a 1.000 Gb.

Con respecto a la capacidad de garantizar la confianza generada, también hay elementos que se deben considerar.

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 al ciento por ciento el carácter definitivo 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 certeza del carácter definitivo de los pagos realizados en cada una de ellas es probabilística[6].

Debido a lo anterior, la firmeza nunca estará garantizada. Para las criptomonedas, cada actualización del registro conlleva una prueba de trabajo adicional que un usuario no honesto 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%.

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 o *forking*, que consiste en un proceso en el que un subconjunto de titulares de una criptomoneda se coordina 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. Este fenómeno ocurrió una vez en 2013 con el Bitcoin y podría volver a ocurrir en el futuro. Las consecuencias de esta bifurcación es que muchas transacciones se pueden anular horas después de que los usuarios las creyeran definitivas.

Como conclusión, las criptomonedas descentralizadas presentan varias deficiencias. Las más importantes se derivan del grado extremo de descentralización: generar la confianza necesaria 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, pero otros parecen inherentes a la fragilidad y la limitada escalabilidad de este tipo de sistemas descentralizados. Esto podría indicar que la deficiencia fundamental de las criptomonedas es precisamente la inexistencia de un mecanismo institucional adecuado a escala nacional.

Otros usos potenciales de la tecnología de registro distribuido

[6] Este problema adquiere mayor relevancia en el caso de las criptomonedas más nuevas, ya que éstas pueden ser manipuladas por un grupo de mineros que controle un porcentaje considerable de la potencia computacional.

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, esta tecnología parece ser eficiente cuando las ventajas del acceso descentralizado superan a los inconvenientes del mayor coste operativo que conlleva mantener múltiples copias del registro. En estos casos se deja de hablar de criptomonedas y se habla de criptopagos, ya que la unidad de cuenta y, en última instancia, el medio de pago de esta plataforma es la moneda soberana.

Una aplicación de esta tecnología es el proyecto sin fines de lucro "*Building Blocks*" del Programa Mundial de Alimentos[7], que gestiona los pagos de ayuda alimentaria destinados a refugiados sirios en Jordania. Este sistema permitió reducir los costos por transacción en aproximadamente el 98% frente a las alternativas basadas en servicios bancarios.

Estos sistemas de criptopagos también pueden resultar prometedores para las transferencias transfronterizas de pequeña cuantía, debido a que los sistemas de pagos internacionales actuales cuentan con múltiples intermediarios, lo que eleva notablemente sus costos. El uso de estos sistemas podría beneficiar en gran medida a aquellos países con gran parte de su población activa en el extranjero.

Por otro lado, algunos protocolos de criptomonedas descentralizadas como Ethereum ya permiten la utilización de contratos inteligentes que ejecutan automáticamente flujos de pagos de derivados. Por lo tanto, el valor agregado de esta tecnología probablemente vendrá dado por la simplificación de procesos administrativos relacionados con transacciones financieras complejas, como el financiamiento del comercio. Lo más importante, sin embargo, es que ninguna de estas aplicaciones precisa el uso o la creación de una criptomoneda.

Desafíos para las políticas económicas

Hoy en día, las autoridades se enfrentan a un importante desafío. Es cierto que su misión es buscar fórmulas para garantizar la integridad de los mercados y los sistemas de pago, proteger a consumidores e inversores y salvaguardar la estabilidad financiera general. Pero, al mismo tiempo, las autoridades deben preservar los incentivos a largo plazo para la innovación y, sobre todo, respetar en todo momento el principio de "a igual riesgo, igual regulación".

[7] La aplicación está bajo el control centralizado del Programa Mundial de Alimentos debido a que las transacciones realizadas en el marco de un experimento inicial basado en el protocolo sin permisos de Ethereum resultaron lentas y costosas

Por lo general, estos objetivos están alineados, pero las criptomonedas generan nuevos retos y pueden obligar a las autoridades a adoptar nuevos enfoques y utilizar herramientas novedosas.

Desafíos regulatorios ante las criptomonedas

El primer gran desafío es la lucha contra el blanqueo de capitales o lavado de dinero y el financiamiento del terrorismo. 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.

Un segundo desafío engloba las normas sobre valores y otras regulaciones que protegen a consumidores y usuarios. 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" o *wallets*, o plataformas de intercambio de criptomonedas. Paradójicamente —y en contraste absoluto con la promesa inicial de las criptomonedas—, muchos usuarios que recurrieron a estos activos por su desconfianza en bancos y gobiernos han acabado confiando en intermediarios no regulados que han resultado ser fraudulentos o han sido víctimas de ataques y robos informáticos.

El fraude es también un problema grave en las ofertas iniciales de criptomonedas (ICO). Una ICO consiste en la subasta pública de una cantidad inicial de criptomonedas y en ocasiones otorga a los compradores derechos de participación en una sociedad *start-up*. Algunas de éstas están vinculadas a proyectos empresariales opacos sobre los que se ofrece información escasa y no auditada, y muchos de estos proyectos han resultado ser esquemas piramidales fraudulentos.

El tercer desafío, a más largo plazo que los dos anteriores, se refiere a la estabilidad del sistema financiero. Aún es incierto si el uso generalizado de criptomonedas y productos financieros de ejecución automática relacionados genera nuevas vulnerabilidades financieras y riesgos sistémicos. Además, dados sus novedosos perfiles de riesgo, estas tecnologías obligan a mejorar la capacidad de reguladores y organismos supervisores.

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 ICO 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 ICO se asemejan a las ofertas públicas iniciales (IPO) 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 ICO 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.

Para articular un enfoque regulador, las autoridades deben considerar tres aspectos de suma relevancia:

- En primer lugar, 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. Debido al carácter global de las criptomonedas, solo una regulación coordinada a escala mundial puede ser eficaz.

- 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 contra el blanqueo de capitales y el financiamiento del terrorismo, la regulación podría centrarse en el punto en el que la criptomoneda se convierte en la moneda nacional.

¿Deberían emitir los bancos centrales sus propias monedas digitales?

Una discusión interesante en el mediano plazo es si los bancos centrales deberían o no poder emitir sus propias monedas digitales (CBDC, por su sigla en inglés), y quién debería poder 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. 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 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 parecer 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 tres importantes ámbitos de intervención de los bancos centrales: los pagos, la estabilidad financiera y la política monetaria. A primera vista, un instrumento de ese tipo traería consigo considerables vulnerabilidades y riesgos financieros, mientras que sus beneficios aún están poco claros.

Por el momento, algunos bancos centrales 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.

Bibliografía

Acuña (2017). Estudio sobre Bitcoin y Tecnología Blockchain. Cuadernos CEF, ESE Business School, Universidad de Los Andes. Disponible en: https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514112818/estudio_sobre_bitcoin_y__tecnolog__a_blockchain.pdf

Auer R. The Mechanics of Decentralised Trust in Bitcoin and the Blockchain, BIS Working Papers.
BIS (2018). Annual Economic Report, June.

Natarajan, H., Krause, S. y Gradstein, H. (2017). Distributed Ledger Technology (DLT) and Blockchain, Grupo del Banco Mundial, FinTech Note, nº 1; BPI.