FACULTAD ECONOMÍA Y NEGOCIOS
UNIVERSIDAD DE CHILE
DEPARTAMENTO DE ECONOMÍA

SERIE DE DOCUMENTOS DE TRABAJO

SDT 521

Las Criptomonedas: Una Mirada Escéptica y los Desafíos a la Industria Financiera y Banca Central

Autores:
José De Gregorio

Santiago, Julio de 2021

sdt@econ.uchile.cl
econ.uchile.cl/publicaciones

Las Criptomonedas:
Una Mirada Escéptica y los Desafíos a la Industria Financiera y Banca Central

José De Gregorio[*]
Facultad de Economía y Negocios
Universidad de Chile

19 de julio de 2021

Resumen

Este trabajo provee un panorama general sobre criptomonedas y los desafíos de las monedas digitales de los bancos centrales. Luego de describir como funcionan las criptomonedas se argumenta que no son y, muy probablemente, nunca serán monedas. Son activos de inversión sin valor intrínseco, es decir, a diferencia del capital que se usa para producir, su uso en producción no existe. A estos activos se les conoce en economía como burbujas especulativas. Que estos criptoactivos no tengan valor no significa que su precio sea cero. Se discuten además algunos problemas de las criptomonedas, como es su uso en actividades ilegales, el elevado consumo de energía y sus implicancias sobre la capacidad de controlar flujos financieros transfronterizos. También se discute la creación de monedas digitales por parte de los bancos centrales, lo que podría reducir los costos de transacción en el sistema financiero, mejorar la seguridad y contribuir a la inclusión financiera. Sin embargo, aún hay muchos desafíos regulatorios y de diseño que resolver.

Keywords: Banca central; burbujas; criptomonedas; criptoactivos; dinero.
JEL Classification Nos. E42; E44; E50

[*] Agradezco los valiosos comentarios y sugerencias de Alejandro Barros, Kevin Cowan, José Tomás De Gregorio, Pablo García, Alberto Naudon, Bernardita Piedrabuena, Camila Russo, Andés Solimano, Pedro Solimano y de manera muy especial a Miguel Musa. Todo el contenido de este trabajo es de mi exclusiva responsabilidad.

1. Introducción

El desarrollo de las criptomonedas en los últimos años ha generado una intensa discusión, así como una curiosidad en los potenciales inversionistas. Por otra parte, la tecnología usada en estos avances tiene múltiples aplicaciones posibles en áreas que van más allá de las finanzas. Incluso, muchos bancos centrales están estudiando la posibilidad de emitir sus propias monedas de manera digital.

Este trabajo pretende dar un panorama general de las criptomonedas y sus perspectivas futuras. En la próxima sección se explica en términos muy simplificados la operación de las criptomonedas, en particular la tecnología de *distributred ledgers* (registros distribuidos) y *blockchain* (cadena de bloques). Luego, en la sección 3, se explican las razones por las cuales las criptomonedas no son, ni probablemente serán, monedas, sino más bien, activos especulativos. El mayor potencial lo podrían tener las *stablecoins*, las cuales atan su valor a monedas regulares, por lo cual tampoco son monedas, sino que certificados respaldados en los activos subyacentes[1]. En la sección 4 se argumenta por qué las criptomonedas son burbujas especulativas, aunque esto no implica que su valor deba ser cero. De hecho, la incertidumbre de su precio es muy elevada, y probablemente siga con alta volatilidad. Luego, en la sección 5, se analizan algunos problemas de las criptomonedas, en particular la preferencia que se tiene sobre ellas para hacer lavado de dinero y otras actividades delictuales, el elevado uso de energía, en particular en el caso de Bitcoin, y sus implicancias sobre los flujos de capitales entre países. La sección 6 extiende la discusión a otras aplicaciones de estas tecnologías en el mundo financiero. La sección 7 está dedicada a la creación de monedas digitales por los bancos centrales. Finalmente, la sección 8 concluye con algunos comentarios finales.

2. La operación de las criptomonedas

El dinero se basa en dos tipos de tecnologías (BIS, 2018). Una, la más antigua, es la de "fichas" (*tokens*). En el mundo moderno, estas "fichas" corresponden a los billetes y monedas, que se traspasan en cada transacción. El riesgo de las fichas es que sean falsas, además no se puede conocer la historia de las transacciones realizadas con una ficha en particular, pudiendo, por tanto, estar ligada a actividades ilegales.

La otra tecnología en que se basa el dinero son las "cuentas". En este caso, hay que verificar que haya dinero en la cuenta, evitando el llamado problema del "doble gasto". Es decir, que una cierta cantidad de dinero se ocupe para gastar dos veces. Las cuentas están centralizadas en los bancos, quienes registran las transacciones y las autorizan en la medida que haya fondos, es decir evitando el doble gasto. Este sistema permite además trazar la

[1] BIS (2019) presenta una definición más amplia de las stablecoins. Pueden atar su valor a monedas específicas, a otros activos como commoditties o incluso otros criptoactivos. También se podría incluir criptomonedas que estabilizan su valor a través de algoritmos por la vía de ajustar la cantidad en circulación (ver Anexo A, BIS, 2019). En todo caso las de mayor desarrollo son las que atan su valor a dinero fiduciario.

historia de las transacciones lo que le permite rastrear operaciones de dudosa legalidad, aunque no siempre con éxito.

Las criptomonedas usan la tecnología de las "cuentas"[2]. Aunque no es equivalente a una cuenta de banco porque no se puede verificar el dueño de ella lo que impide a las instituciones financieras cumplir con la regulación de *know your* customer (KYC), que se discute en la sección 5. La verificación de la cuenta se hace de manera descentralizada y segura, en todos los nodos de la red, evitando el problema del doble gasto, pero sin recurrir a una institución central que lo valide. Esto lo hace, además, muy seguro. De esta forma, las transacciones son completamente trazables, pero anónimas.

Las cuentas se denominan "billeteras", a las cuales se puede acceder con dos claves, una pública y una privada. Esta última la tiene solo el dueño de la billetera. Las cuentas son identificadas en la red mediante la clave pública que consiste en una expresión alfanumérica. No hay otro registro que permita dar con la identidad real del(los/las) propietario(s), lo que sirve para resguardar el anonimato. En efecto, el anonimato es una característica fundamental de las criptomonedas y esto explica por qué son el medio preferido para muchas transacciones ilegales. Es posible en todo caso, algo que pueden hacer bancos centrales con sus monedas digitales, crear monedas donde la identidad del dueño de la billetera sea conocida.

Para acceder a las billeteras, cada una de estas cuentas tiene una clave privada –generada a través de criptografía[3] por la clave pública– por medio de la cual su propietario puede ordenar transferencias directas de criptomonedas de una billetera a otra. Esto es equivalente a un lo que en la actualidad existe en muchos sitios de internet, un *username* (clave pública) con un *password* (clave privada). Dicha clave privada solo es conocida por el propietario de la billetera y se usa para firmar, acceder a la billetera y dar órdenes de pago. La pérdida de esta clave representa la pérdida de la billetera y todo lo que ella contiene.

Las transacciones se realizan dando órdenes de pago desde una billetera digital a otra. Estas transacciones se pueden realizar directamente entre dos individuos, o se pueden hacer a través de una plataforma de transacciones de criptomonedas. La plataforma permite además, realizar operaciones de cambio entre criptomonedas y monedas de curso legal, como el dólar estadounidense o el peso chileno.

[2] Se puede también argumentar que son "fichas", y que la historia de las transacciones es para verificar la validez del Bitcoin, así como con billetes se revisa la autenticidad de este.

[3] La criptografía es una técnica con orígenes muy antiguos que permite encriptar mensajes, de manera que solo quien conoce las claves puede desencriptarlos. Una técnica simple de encriptación, por ejemplo, es cambiar las letras una a una. En la actualidad, la criptografía se usa mucho en computación y se basa en matemáticas muy complejas, donde a un conjunto de datos se le asigna un resultado único que es otro conjunto de datos. Las matemáticas permiten también recuperar el conjunto de datos originales, es decir, desencriptar, pero no necesariamente con ello se conoce la fórmula que generó los datos.

Por otra parte, la verificación de las transacciones en criptomonedas es descentralizada y segura. No existe una entidad central que valide las transacciones. La verificación de las criptomonedas se basa en un registro distribuido *(distributed ledger)* entre todos los participantes, donde se van validando y agregando todas las transacciones en forma secuencial. Es decir, cada nodo tiene toda la historia de las transacciones, de manera que esta historia está guardada en muchos computadores, lo que, unido a las complejidades criptográficas, la hacen inviolable. Si alguien lograra cambiar un registro a través de criptografía reversa, lo que ya es prácticamente imposible, el resto de los nodos lo rechazaría[4].

Supongamos por ejemplo que "A" va a transferir cierto monto de Bitcoin a "B". Desde su billetera digital, A da la orden de transferencia a la clave pública de B. Esta orden se transmite a todos los nodos de la red. En dichos nodos, los mineros[5] "excavan la orden" para resolver el problema criptográfico de las transacciones aún no validadas. El primer "minero" que resuelve el problema recibe un premio, que es el incentivo por validar transacciones.

Una vez que un "minero" resuelve el problema (conocido como "prueba de trabajo"), empaqueta las transacciones recién validadas en un bloque y lo agrega al final de la cadena que registra todas las transacciones anteriores. Esta cadena de bloques o *blockchain* es pública, de modo que el resto de los "mineros" puede verificar que esta solución es correcta. Esto es lo que genera consenso en la red, evita el "doble gasto" y permite ir agregando bloques a la cadena, los que no se puede modificar posteriormente. Estas cadenas de bloque constituyen los registros que se distribuyen a través de la red[6].

En el caso del Bitcoin, el premio al "minero" por resolver el problema criptográfico consiste en que nuevos Bitcoins son creados y se le otorgan a dicho "minero". Estos premios han ido cayendo gradualmente en el tiempo, pues el creador de Bitcoin estableció un límite de 21 millones de Bitcoins, a fin de evitar la emisión ilimitada de dicha criptomoneda (*debasing*)[7]. Sin embargo, si se convirtiera en medio de pago, al alcanzar su máximo de emisión y la demanda por dinero sigue subiendo producto del crecimiento, debiera haber deflación en bitcoins, lo que no es algo deseable. Si aparecen nuevas monedas para acomodar el crecimiento tendrían riesgo de *debasing*, lo que podría causar una hiperinflación en bitcoins, es decir llevar su valor a cero.

[4] Sin embargo, existen dudas si será posible para los futuros "quantum computers" desencriptar con cierta facilidad (IOSCO, 2017).

[5] Se entiende por "mineros" a los operadores de los nodos de la red, quienes trabajan en resolver los problemas criptográficos que validan las transacciones de criptomonedas.

[6] Existen muchas tecnologías que pueden constituir registros distribuidos, el *blockchain* es una de ellas, y tal vez la más popular.

[7] En la actualidad, hay unos 19 millones de bitcoins emitidos. Una vez alcanzado el límite, los mineros debieran empezar a recibir sus pagos por la vía de comisiones.

Una ventaja de Bitcoin es que no hay costos de transacción relevantes[8]. Sin embargo, una vez que se llegue a su límite máximo no habrá premio para los mineros que validen las transacciones. En ese momento deberán cobrar comisiones para mantener operando la minería, y estas pueden llegar a ser relevantes. Es necesario dar incentivos a los mineros que validan transacciones y dado los costos de energía actuales de resolución de las pruebas de trabajo en Bitcoin, esto costos podrían ser significativos.

3. Las criptomonedas: no son dinero, son activos

El dinero es normalmente definido por sus funciones. Estas funciones son tres y deben ser cumplidas por cualquier tipo de dinero[9]:

- *El dinero es una unidad de cuenta*: los precios se fijan en términos de dinero. Existen otras unidades de cuenta, en Chile por ejemplo hay unidades indexadas al índice de precios como son la UF (unidad de fomento) y la UTM (unidad tributaria mensual), pero dichas unidades no cumplen con las otras funciones del dinero. Además, al estar indexadas a algún dinero, no son unidades de cuenta en si mismas. Para que sea unidad de cuenta efectiva es indispensable que tenga un valor estable. Eso es precisamente lo que hace el Banco Central para que su moneda nacional sea útil, le da estabilidad a su moneda. La UF y la UTM al estar indexada al valor de una moneda estable también pueden cumplir el rol de unidad de cuenta porque la moneda subyacente tiene un precio estable.

Esto no ocurre con las criptomonedas, pues si algo no han tenido es estabilidad de precios[10]. Difícilmente alguien fijará precios en criptomonedas. Por ejemplo, considere a alguien que a principios de 2021 quiere vender un bien inmueble en Chile en 5000 UF, esto hubiera sido el equivalente a 145 millones de pesos, y al valor del Bitcoin y dólar al primero de enero, el precio en Bitcoin sería 7.07[11]. Si se anunciara el precio en Bitcoin, es decir 7.07, el valor del inmueble hubiera subido de 145 a 314 millones de pesos a mediados de abril. Difícilmente alguien hubiera usado el Bitcoin para fijar el precio del inmueble.

Un aspecto fundamental de una moneda ampliamente aceptada es que su valor sea estable y este no es el caso del Bitcoin ni de ninguna criptomoneda de precio variable. No es este el caso de las llamadas *stablecoins,* cuyo precio está atado a monedas regulares y no son

[8] Actualmente hay costos de transacción, los que son bajos respecto del costo energético aunque bastante volátiles.

[9] Ver, por ejemplo, De Gregorio (2007), cap. 15.

[10] Esta volatilidad existe también con monedas nacionales de curso legal, las que debido a hiperinflaciones no cumplen con la estabilidad de su valor, lo que obviamente cuestiona el hecho que sean monedas. En la hiperinflación de Zimbawe antes de la abolición del dólar de Zimbawe se permitió el uso de dólares estadounidenses para transacciones. En países que experimentan hiperinflaciones sus monedas se dejan de usar, y se podría concebir que los criptoactivos puedan cumplir un rol como medio de pago e unidad de cuenta, sin embargo en este trabajo se consideran monedas de valor estable y predecible.

[11] Para lo ejemplos se usará por lo general el Bitcoin, la criptomoneda más usada. Un 41% de la capitalización de mercado a junio de 2021 era el Bitcoin, seguida por Ethereum con un 19%.

monedas por otras razones a que me referiré más adelante. Si el Bitcoin fuera la moneda que remplazara al dólar, el año 2018 la inflación hubiera sido 270% y el año 2020 una deflación de 75%. Claramente con esa volatilidad no podrá ser nunca una moneda, solo será un activo.

- El *dinero es un medio de pagos*: Los pagos por los bienes se realizan intercambiando bienes por dinero. Para esto, la estabilidad de precios es también importante. Si se cierra un negocio y los pagos ocurren después, realizar este pago en dinero no es mayor problema. En cambio, la volatilidad de los precios de las criptomonedas no las hace convenientes para se usadas como medio de pago. Tampoco su velocidad de validación de transacciones.

Volviendo al ejemplo del bien inmueble. Suponga que el precio se fija en el equivalente a 145 millones de pesos al 15 de abril, es decir 3,26 bitcoins. Si mientras revisa papeles y junta el dinero se demora quince días, el comprador, al nuevo valor del bitcoin y el dólar, pagaría 134 millones de pesos. Al vendedor le convendría deshacer el negocio, e incluso pagar un costo por romper el contrato. Por lo tanto, el Bitcoin no sería una unidad atractiva para escribir el contrato y realizar los pagos. La incertidumbre es muy alta.

Uno podría hacer el pago en criptomonedas al valor del momento en que se realiza el intercambio, en ese caso es exactamente lo mismo que pagar con acciones o cualquier valor con precio de mercado. Pero no es un medio de pago que pueda ser generalizado.

- *El dinero es un depósito de valor*. Esto significa que el dinero sirve para traspasar valor a través del tiempo. Existen muchos instrumentos para ahorrar, pero un depósito de valor debe proveer un valor estable a través del tiempo, algo que la volatilidad del precio de las criptomonedas no estables, como el Bitcoin, no pueden ofrecer.

Las criptomonedas sirven para ahorrar, al igual que las acciones, bonos, o cualquier otro activo. Por lo tanto, dado que las criptomonedas no son dinero, sino que un activo, no es correcto llamarlas así. Es más adecuado hablar de criptoactivos, con una elevada volatilidad.

Una forma de estabilizar su precio es fijarlo respecto a una moneda estable. Esto es lo que hacen las *stablecoins* más usadas. Por ejemplo, Tether es una criptomoneda que se cambia uno a uno con el dólar. Evita la volatilidad, pero no es una moneda con vida independiente, pues debe estar completamente respaldada por dólares, o sea para emitir la criptomoneda hay que adquirir dólares, de manera que el activo subyacente es el dólar. El valor de la moneda es dado por la moneda subyacente y su oferta está determinada por el banco central de la subyacente. Tal como los regímenes de cambio fijo. Es como tener una cuenta en dólares en el banco, pero con la tecnología de criptomonedas[12].

[12] Seguiré usando la expresión criptomoneda porque es su acepción más usual, aunque no significa que acepte que es una moneda porque, como se argumenta en el texto, no lo es.

Tether es la tercera moneda digital, con una capitalización de 63 mil millones de dólares. Podría tener ventajas por su facilidad para transar y realizar pagos en dólares, con los consecuentes riesgos en materia de flujos de capitales entre países que se discute más adelante. Además, existe un problema serio de fe pública en las *stablecoins* pues es necesario asegurarse que el respaldo existe[13]. De hecho Theter fue recientemente multado en Nueva York porque no informaba adecuadamente tener todas sus monedas respaldadas. En todo caso, estas monedas estables podrían proveer un beneficio muy grande. Por ejemplo, en facilitar transferencias de migrantes a sus países, sin los abismantes costos de transacción actuales. Pero el costo es que estará fuera de cualquier regulación, control de flujos de capitales y no hay protección al usuario.

A mediados de 2019 Facebook anunció el lanzamiento de Libra, una criptomoneda basada en cadenas de bloques y cuyo valor está fijo a una canasta de monedas. Tampoco es una moneda solo un vehículo para facilitar transacciones. Libra se pasó a llamar Diem, y aún no ve la luz.

En resumen, el objetivo por el cual el Bitcoin fue creado no se ha cumplido, no es una moneda. Más aún, en 2019 solo el 1,3% de las transacciones de Bitcoin fueron con comercios, el resto fueron operaciones financieras. El número de transacciones al día de Bitcoin alcanzó a 330.000 en diciembre de 2020. En cambio, las transacciones de tarjetas de crédito por día solo en los Estados Unidos en 2019 fueron 108 millones, es decir 325 veces más.

Otro problema de las criptomonedas es el tiempo que se demora en validar las transacciones con las tecnologías vigentes. En la actualidad está en torno a 10 minutos. ¿Se imagina esperando en una caja de supermercado 10 minutos para que le validen la transacción? En el caso de las tarjetas de crédito la validación de la transacción es instantánea, salvo demoras de conexión. El sistema que soporta Bitcoin puede procesar 7 transacciones por segundo, mientras Visa procesa 60.000.

Hay plataformas privadas muy rápidas en transacciones, pero, en la medida que se masifiquen las pruebas de trabajo, se pueden volver más lentas. Existen también algoritmos alternativos a la prueba de trabajo que pueden aumentar notablemente la cantidad de transacciones por segundo, pero en general estas operan en plataformas privadas, dado que estos algoritmos son menos descentralizados, y estas plataformas deben ser operados centralizadamente por una o un conjunto de entidades.

[13] Hay criptomonedas que estarían mejor auditadas, como USDC, pero aún respaldadas uno a uno con monedas regulares. También hay criptomonedas como Dai, que se fija iguala un dólar y cuyo respaldo es en criptoactivos. Al momento de escribir este trabajo tendría respaldo de 3 dólares por Dai. Sin embargo, si el valor de esos criptoactivos, cuyo precio es variable, colapsa, también colapsará en Dai.

Existen tecnologías que podrían acelerar la validación de transacciones. En 2015 se propuso la *Lightning Network*, como una segunda capa a la red de Bitcoin para pagos de bajo valor. Básicamente consiste en un canal privado, por ejemplo, los clientes de un café. Ellos depositan bitcoins en ese canal y hacen transacciones instantáneas, y solo cuando el canal se cierra se entra al proceso de prueba de trabajo de Bitcoin[14]. En abril de 2021, solo un 2% de los nodos de la red de Bitcoin admiten la segunda capa.

4. Las criptomonedas son burbujas especulativas

¿Cuál es el valor de las criptomonedas? La mayoría de los activos son un derecho sobre algún subyacente. Por ejemplo, una acción es un derecho sobre las utilidades de una empresa. Los bonos, son un derecho sobre un flujo de pagos futuros. Una casa es un derecho sobre el valor de vivir en ella, o de su arriendo.

No obstante, las criptomonedas no tienen ningún activo subyacente. Son activos sin valor intrínseco, solo vale porque existe la confianza que otros lo valoran y están dispuestos a comprarlo. En economía, a ese tipo de activos se les llama *burbujas*. Los activos con valor intrínseco también pueden tener una parte de burbuja. De hecho, en dichos casos, se dice que los activos tienen un valor *fundamental*, basado en el valor de los derechos sobre flujos futuros que tiene, y un componente de *burbuja* que no se puede explicar por los fundamentos. Las casas durante la crisis *subprime* de 2008-09 tenían burbujas en sus precios, al igual que las acciones tecnológicas durante la burbuja de las *dotcom* de fines de los 90.

El dinero también es una burbuja, pues no tiene un valor intrínseco y la gente lo valora porque confían que el resto de la economía lo acepta.[15] Que sean monedas de curso legal, garantizadas por el estado, y los bancos centrales ajusten la oferta y lo hagan de manera creíble que permite que su valor sea estable, las convierte en monedas.

¿Que un activo sea una burbuja significa que su precio de largo plazo debiera ser cero? No necesariamente. Si existe demanda por el activo su precio no debe ser cero. El Bitcoin y las criptomonedas podrían ser el "nuevo oro" (Tirole, 2017), un activo que se demanda porque no está correlacionado con la inflación ni el ciclo económico mundial. Similar al oro, que se usa como activo de protección, aunque su retorno ha sido muy bajo, cercano a la inflación, y ello explica entre cosas el por qué los bancos centrales lo han dejado de usar como activo de reserva. Pero tampoco se puede descartar que su valor vaya a cero, que es su valor fundamental.

[14] Esto es similar a las tarjetas de prepago que funcionan offline en el día y la liquidación se realiza en la noche.

[15] De acuerdo con la teoría el dinero podría perder todo su valor, como cualquier burbuja cuando colapsa, lo que produciría una hiperinflación. Para evitar que eso suceda basta que haya algún respaldo fiscal a la moneda, incluso incierto, lo que de hecho existe y es por eso que no se observan hiperinflaciones sin causas fiscales. Ver Obstfeld y Rogoff (2021).

¿Es irracional comprar Bitcoins? No, como ya he señalado, puede ser una burbuja especulativa plenamente racional y tener un valor positivo y elevado, pero resulta imposible tener alguna noción de a que valor podrá llegar pues no tiene valor fundamental. En todo caso, el riesgo es muy alto, porque tal como sucedió desde que se conocen la existencia de las burbujas, empezando por el caso de los tulipanes en Holanda en el s. XVII, su precio puede caer a un nivel cercano a cero[16]. No obstante, aunque no hay información definitiva sobre la duración de las burbujas, la del Bitcoin debe ser la más larga y puede durar mucho más, pero es técnicamente una burbuja.

¿Es el Bitcoin un esquema Ponzi? No. Un esquema Ponzi es una pirámide en el cual se promete un retorno que se va pagando con el ingreso de nuevos inversionistas. Este esquema colapsa tarde o temprano, ya que en algún punto dejan de entrar inversionistas. Esto no ocurre en el mercado de criptomonedas. Pueden entrar nuevos inversionistas y hacer subir el precio, pero aquí no hay seguridad de retorno, nadie es estafado si su precio va a cero, más aún su precio puede seguir subiendo como una burbuja sin que haya nuevos inversionistas.

5. Los riesgos y costos

Es importante destacar que el uso de criptomonedas tiene un conjunto de riesgos que es necesario tener presentes, tanto para los usuarios como para las autoridades regulatorias.

5.1 Lavado de dinero y actividad delictual

La mayor ventaja de Bitcoin es que es seguro, trazable y anónimo, siendo este último elemento su mayor riesgo desde el punto de vista social. Este es el caso de rapto de sistemas computacionales (*ransomware*) y otras actividades delictuales. De hecho, el reciente rescate de los sistemas de la empresa Colonial Pipeline se hizo en criptomonedas, pero por un monto fijado en 4,4 millones de dólares.[17] Todos los casos conocidos han envuelto el pago en criptomonedas, aunque su precio sea fijado en dólares u otra moneda. Otro problema con los raptos cibernéticos es que no tienen fronteras debido al uso de criptomonedas, lo que hace aún más complejo su rastreo.

Los anterior pone un problema complicado para los sistemas financieros, donde la regulación KYC (*know your customer*) es importante, algo que no se puede asegurar de las operaciones en criptomonedas. Por lo tanto, las entidades reguladas tienen serios problemas para operar en criptomonedas en las cuales las identidades no sean conocidas, aunque podrían aparecer monedas que terminen con el anonimato.

[16] Para la teoría de burbujas en economía ver Brunnermeir y Oehmke (2013) y para la historia de las primeras burbujas en el mundo ver Garber (1990).

[17] No se conocen detalles de la operación, pero todo indica que el rescate se fijó en dólares, pero el pago se hizo en criptomonedas porque ellas permiten el anonimato.

Hay quienes pueden argumentar que Bitcoin es pseudo-anónima pues siempre es posible conocer las identidades, en especial cuando salen del sistema para comprar bienes y servicios. Una vez que una moneda entra en transacciones toda su historia queda registrada en los registros distribuidos y públicos. Pero como se documentó antes son muy pocas las transacciones en Bitcoin para compra de bienes y servicios, además el cambio por monedas regulares puede realizarse en jurisdicciones que no compartan internacionalmente su información de actividades ilegales.

Ha sido posible rastrear transacciones del pago del rescate de Colonial pipeline, y se ha podido recuperar parte del rescate. Esta es una operación compleja y costosa, y difícilmente se puede pensar que el rastreo y capacidad de detectar a los raptores se puede hacer de manera frecuente. Asimismo, ha aparecido una criptomoneda nueva, Monero, que asegura la imposibilidad de trazabilidad, y parte de los pagos del rescate se hicieron en esta moneda. No es sorpresa entonces que el precio de Monero haya aumentado más que el de Bitcoin durante este año.

Es complejo tener una estimación de las actividades ilegales con Bitcoin. Usando algoritmos sobre las cadenas de bloques existentes, búsquedas en la *darknet* y datos oficiales Foley et. Al (2021) concluyen que, entre 2009 y 2017, un 46% de las transacciones en Bitcoin son ilegales, cercano a la escala del mercado de drogas en Estados Unidos y Europa. Sin embargo, esto representa solo a un 6% de los participantes en Bitcoin, en consecuencia, se puede asegurar que una pequeña fracción de los usuarios son quienes realizan una gran fracción de las operaciones ilegales[18].

Otro problema con el anonimato de Bitcoin es la evasión de impuestos. Recientemente en Corea las autoridades confiscaron criptoactivos a 12.000 personas acusadas de evasión de impuestos.[19] El anonimato y las dificultades de rastrear la identidad de las cuentas crea un espacio relevante para evasión de impuestos. Por ejemplo, alguien que compra y vende criptomonedas con ganancias de capital podría evadir los impuestos sin declararlos. Se les puede exigir a las plataformas de transacciones que informen todas las ganancias de capital en sus cuentas, como ocurre con los intermediarios financieros. Sin embargo, esto no se puede hacer cuando las transacciones son P2P (*peer to peer*).

Otro problema de las criptomonedas en esta área son los riesgos operacionales y exposición a fraudes. De hecho, en las plataformas se opera entregando las claves privadas, lo que las hace susceptibles de *hackeo*, como ya ha ocurrido. Esto pudiera requerir de algún grado de regulación para protección de los clientes financieros.

[18] No hay estudios recientes de que está pasando con el volumen de transacciones ilegales. De acuerdo con un informe de un ex subdirector de la CIA para una agencia de lobby de criptomonedas los delitos cometidos con Bitcoin estarían cayendo de manera importante y yéndose a otras criptomonedas que ofrecen más privacidad como Monero. En todo caso en Bitocin.org ofrecen sugerencias a través del uso de varias billeteras para proteger el anonimato.

[19] Para otras estimaciones de montos envueltos en raptos cibernéticos ver Pacquet-Clouston et al. (2019).

5.2 Uso de energía

La actividad minera de criptomonedas es muy intensiva en energía. Se necesitan grandes servidores con mucho poder computacional para resolver los problemas criptográficos requeridos para las *pruebas de trabajo*, lo que obviamente tiene consecuencias medio ambientales importantes.

El Centro Cambridge de Finanzas Alternativas, de la universidad del mismo nombre, ha estimado que Bitcoin consume 130 Terawatt hora por año, mayor al consumo de países como Suecia o Noruega. En todo caso no se conoce cuanto de esta energía es intensiva en carbón, por lo tanto, no hay datos sobre su huella de carbono. Por ejemplo, tiene algunas ventajas instalarse en lugares fríos para ahorrar en aire acondicionado, algo que no usa carbón intensivamente. Pero, si la energía es de bajo costo en países contaminantes, también hay incentivos para instalarse ahí.

Se ha argumentado que la minería de Bitcoin usa menos energía que otras industrias. De acuerdo a Galaxy Digital, la minería de Bitcoin usaría menos de la mitad del uso de la industria bancaria. Sin embargo, la estimación relevante debería ser el consumo de energía por unidad de valor agregado. En Estados Unidos la industria financiera es en torno al 7% del PIB, en cambio si el Bitcoin es un activo financiero sin valor intrínseco su valor agregado sería muy bajo, probablemente cero. En consecuencia la razón de uso de energía a valor agregado tendería a infinito. Al menos, sería difícil encontrar a alguien que se atreviese a afirmar que en alguna mínima fracción el valor agregado de las criptomonedas se acerca al PIB de Suecia.

En un reciente comunicado del G7, donde se declara que se trabajará en monedas digitales entre bancos centrales, se establece que este trabajo debiera ser eficiente en materia energética.

En la actualidad se está trabajando en una tecnología que remplace a la prueba de trabajo para ahorrar en energía. Esta se conoce como la prueba de participación (*proof of stake*), la que selecciona a los nodos que validan las transacciones basado en la participación de ese nodo en el valor total de la criptomoneda. Se entiende que quienes tienen más participación en la moneda tienen también los mayores incentivos para que el sistema funciones bien. En vez de una competencia por poder computacional que consume mucha energía en la prueba de trabajo, la prueba de participación que asigna aleatoriamente la validación usaría mucha menor energía. Esta tecnología que aún está en desarrollo y tendría el potencial de ser más amigable con el medio ambiente.

5.3 Controles de capital

Un tema muy discutido en economías emergentes es el uso de controles de capital para regular las entradas y salidas de capitales. Con las criptomonedas esto no es posible. Es imposible también prohibirlas, seguirán existiendo en el mundo digital. Si alguien quiere

sacar capitales de una economía, puede usar moneda local para comprar criptomonedas. Luego estas criptomonedas se venden en el país hacía donde se quieran sacar los capitales, o simplemente transformarlos fuera de las fronteras en la moneda deseada. No queda registro de la transacción transfronteriza.

Podríamos llegar a la extraña situación en que las autoridades ponen controles en todos los flujos legales y regulados, mientras tienen una actividad paralela, sin regulación, que podría hacer todo tipo de arbitrajes. En definitiva, las criptomonedas imponen un serio desafío para las autoridades no solo en materia de regulación, sino también para tener información de los flujos de capitales.

6. La revolución tecnológica en el mercado financiero

La tecnología de las criptomonedas, blockchain, y todos los desarrollos en la industria financiera que usan tecnologías nuevas (conocido como *FinTech*) son tal vez el mayor cambio financiero ocurrido en décadas. Ha sido disruptivo y llegó para quedarse. También abre un abanico de oportunidades y riesgos que es necesario abordar.

Las cadenas de bloques pueden usarse en muchas aplicaciones y daría seguridad y eficiencia. Por ejemplo, se podría tener todo el catastro de propiedades en un registro distribuido, ahorrando en intermediarios y trámites para sus transacciones. En vez de gastar días y recursos en conseguir papeles, todo podría estar validado y seguro en dichos registros. La información médica y muchas otras, podrían digitalizarse y así como hoy en internet operamos con muchas claves, en el futuro todos podríamos tener nuestra clave criptográfica, y en el caso de Chile basada en el RUT.

Mención especial merece Ethereum, la segunda en capitalización después de Bitcoin[20], cuya moneda digital es Ether. Ethereum fue quien lanzó los trabajos para la prueba de participación que reduciría los requerimientos energéticos que usa la prueba de trabajo.

Es mucho más que una criptomoneda, es una plataforma que provee la posibilidad de crear muchas aplicaciones con la tecnología de cadenas de bloques. Como estas aplicaciones usan tecnología de cadenas de bloques, una vez validadas no se pueden eliminar ni cambiar. La más conocida es la posibilidad de escribir contratos. Estos contratos se conocen como *contratos inteligentes* (*smart contracts*) y potencialmente pueden tener muchas aplicaciones. El contrato especifica condiciones y cuando estas condiciones se cumplen se efectúan los pagos o se gatillan otras acciones automáticas. Un caso sencillo sería usarlo en apuestas, donde el ganador es fácil de verificar, lo mismo con contratos de arriendo y pagos. Es similar a una cuenta *escrow*, pero en este caso es digital y no bancaria[21]. Es aún una tecnología nueva, pero con mucho potencial, ya que puede reducir costos de

[20] Para más detalles ver Russo (2020)

[21] Las *escrow accounts* son cuentas depositadas con terceros que se liberan una vez que ciertas condiciones pre acordadas se cumplen.

intermediación y fraude, y además es muy segura. La plataforma también se usa para levantar fondos que financien inversiones, saltándose el mercado de capitales tradicional, y emitiendo como respaldo una moneda en un ICO (*initial coin offering*). La moneda pasa a ser más bien una acción. Obviamente hay problemas de fe pública y protección del consumidor en estos temas, por eso las emisiones de acciones son muy reguladas. En los ICO puede haber estafas.

En todas las aplicaciones de Ethereum se puede usar Ether para la liquidación de pagos, aunque persiste el problema que es muy volátil, por lo cual hace que su uso para pagos futuros es incierto. No obstante, los contratos no solo se pueden escribir con pagos en Ether sino que también en monedas verdaderas.

Los contratos inteligentes son parte de una tendencia mayor llamada DeFi (*decentralized finance*), y que Ethereum fue un impulsor importante. Usa las tecnologías de registros distribuidos y cadenas de bloques. El objetivo de DeFi es replicar las funciones que realizan los sistemas financieros, pero de manera descentralizada y digital[22]. Por ejemplo, en el corretaje de valores. Las custodias podrían hacerse de manera descentralizada. Se pueden otorgar créditos, manejo de activos y muchos otros servicios financieros. Sin embargo, hay muchos temas regulatorios pendientes como es la protección del consumidor, la protección de datos personales, la continuidad operacional y los riesgos financieros, entre otros, que es indispensable abordar.

Las plataformas de *blockchain* fueron creadas como respuesta a la necesidad de mayor privacidad. Con los *Smart contracts* han surgido un conjunto de aplicaciones privadas usando esta tecnología, por ejemplo, Corda y Quorum. Estas plataformas privadas sacan provecho de las características de *blockchain*, como su capacidad de crear ecosistemas y preservar la inmutabilidad y seguridad, pero sin la necesidad de utilizar plataformas públicas que tienen menor capacidad de procesamiento.

Esta revolución digital en finanzas tiene muchas posibilidades de mejorar la inclusión financiera, proveyendo servicios simples y a bajo costo. Sin embargo, muchas compañías de FinTech están capturando muchos datos de sus clientes sin su consentimiento, o, al menos, que esta privacidad este debidamente resguardada. De hecho, esa es la remuneración de algunas FinTech[23]. Obviamente esto tiene importantes implicancias sobre la privacidad de datos (Adrian y Mancoini-Griffoli, 2021).

7. Las monedas digitales de los bancos centrales

Los bancos centrales no se han quedado fuera del desarrollo de criptomonedas[24]. Las inquietudes que las criptomonedas puedan remplazar a las monedas nacionales, con la

[22] Para más antecedentes ver WEF (2021).

[23] Esto no ocurre en DeFi porque no se entregan datos personales, es anónimo.

[24] Para una completa discusión sobre CBDC ver el Auer y Bhöme (2020), Bank of England (2020) y el capítulo III de BIS (2021).

consecuente pérdida de capacidad de hacer política monetaria y recaudar señoreaje, así como el aprovechamiento de las nuevas tecnologías para crear dinero, han sido tal vez los principales motivos detrás de este interés. Aunque no creo que las criptomonedas tengan chance de remplazar las monedas nacionales, los riesgos que ello ocurra requieren de darle prioridad a estos temas. Por otra parte, es necesario que las autoridades monetarias y financieras tengan pleno conocimiento de las tecnologías y su aplicación para el bienestar de la población, en especial en lo que se refiera a inclusión financiera. Pero también es indispensable que las autoridades monitoreen estos desarrollos por sus implicancias para la regulación y la estabilidad financiera. La existencia de criptomonedas privadas podría también generar problemas de flujos transfronterizos y volatilidad de los tipos de cambio que requieren atención de las autoridades.

Pero también las nuevas tecnologías pudieran generar beneficios para la ciudadanía a través de la generación de un sistema de pagos que ofrezca la simplicidad del uso de efectivo y al mismo tiempo sea seguro y eficiente. Las monedas de los bancos centrales podrían producir muchos beneficios en materia de inclusión financiera. Las transacciones en monedas digitales son instantáneas, funcionan como efectivo, a diferencia de pagos con tarjeta, transferencias y otros que tienen costos de transacción y además tiempos de espera mientras se espera que las transacciones se validan y los fondos se transfieran.

A estas monedas se les conocen como CBDC (*central bank digital currency*). La mayoría de los bancos centrales están en la "prueba de concepto" respecto de criptomonedas y todos estudian las posibilidades de implementación.

Avanzar en monedas digitales o tecnologías que reduzcan los costos de transacción es un desarrollo muy positivo. En muchos países, el sistema de transferencia entre cuentas bancarias es lento, engorroso y caro. Para una empresa pequeña es bueno disponer de los fondos lo antes posible y transferencias instantáneas serían deseables. Las transferencias internacionales son también engorrosas y caras en la mayor parte del mundo. Las monedas digitales de los bancos centrales pueden proveer un importante beneficio a la economía. Sin embargo, existen muchos problemas de compleja solución que aún se deben resolver.

En el caso de Chile el sistema de transferencias es rápido y gratuito. Esto abre la pregunta de cuando debiesen apostar las autoridades chilena por sistemas descentralizados versus seguir fortaleciendo sistemas electrónicos centralizados sobre las cuentas de los bancos privados u otros emisores. Probablemente las monedas digitales descentralizadas tengan mayor potencial en transacciones transfronterizas de bajo valor.

Otra aplicación interesante de las criptomonedas de los bancos centrales es que este dinero puede ser programable y así, por ejemplo, si el gobierno quisiera repartir cajas de alimentos durante una pandemia, podría ser más eficiente y rápido entregar bonos de dinero digital para uso exclusivo en alimentos.

Obviamente los bancos centrales no proveerán monedas con fluctuaciones de precios como Bitcoin y por ello se podrían adoptar las tecnologías de los *stablecoins* para ofrecer medios de pago por la vía de *blockchain*. Los bancos centrales podrían ofrecerle al público billeteras digitales para mantener el dinero. Sin embargo, esto podría crear desintermediación con el sistema bancario y su función de transformación de madurez (financiarse con depósito—dinero—y prestar a más largo plazo) y otorgamiento de crédito. El banco central no puede dedicarse a hacer préstamos e incurrir en riesgo de crédito. ¿Cómo canalizarán los fondos para que sean prestados? ¿Los licitarán? En todo caso, aunque las cuentas corrientes y depósitos vista son sólo una fracción del fondeo de los bancos estos problemas podrían limitar la intermediación financiera con consecuencias negativas sobre la economía. Otra pregunta relevante en el mundo de monedas digitales es quienes tendrán acceso al banco central como prestamista de última instancia. Adicionalmente, otro inconveniente, es el uso de la electricidad para las pruebas de trabajo en las transacciones.

No es necesario que las CBDC sean completamente descentralizadas, que son las que necesitan algoritmos que consumen mucha energía para validar transacciones. Se podrían usar plataformas privadas en donde hay validadores autorizados, en un caso extremo podría ser el banco central el único validador, o se pueden usar algoritmos rápidos como es la *proof of authority*, llamada así porque hay solo algunos nodos que son los autorizados a validar. Es este el camino más probable que se siga con los CBDC.

Otra dificultad que pueden encontrar las CDBC son los problemas de violación de la privacidad. Un desarrollo en sus primeras etapas que podría resolver esto son modelos de privacidad asimétrica (Tinn and Dubach, 2021). Por ejemplo, todas las personas tendrían dos billeteras, una anónima y otra que cumple con condiciones de KYC de regulación financiera. Todas las transferencias deben llegar a la billetera no anónima, pero las transferencias se podrían hacer de cualquiera de las dos billeteras. Desde el punto de vista de impuestos y regulación lo más relevante es identificar al receptor, no el originador.

Existen otros problemas complejos de las criptomonedas, *stablecoins* en particular, en comparación a los CBDC. Las monedas de los bancos centrales son un pasivo del banco, que asegura que será aceptado como medio de pago, no hay riesgo de estafa, y las cuentas en el sistema bancarios están aseguradas. Nada de eso ocurre con los *stablecoins*. Nada asegura que tengan el suficiente respaldo de sus monedas. Tal como sabemos de la literatura de colapsos de tipo de cambio fijo, podría haber una corrida contra una moneda y provocar serios problemas, además de fraude. Si las plataformas de monedas digitales son *hackeadas*, nadie es responsable. No así con las cuentas bancarias y todas aquellas que están dentro del perímetro regulatorio de las autoridades.

Una historia interesante es de la corredora *Quadriga* de Canadá. Su dueño falleció en 2018 y las claves criptográficas de las billeteras, así como las de su computador solo las conocía él. Se estima que se perdieron alrededor de 200 millones de dólares de 115 mil clientes. Este era además un juego Ponzi pues se determinó que su dueño desvío fondos a sus

cuentas personales, y los requerimientos de los clientes eran cubierto con el dinero de nuevos clientes que conseguía su corredora.

Las CBDC podrían constituirse como un sistema de dos partes, en el cual se mantiene la forma actual de distribución de dinero. El banco central emite CBDC solo a entidades financieras reguladas, y dichas entidades les ofrecen billeteras digitales a sus clientes (Bank of England, 2020). Asimismo, se podría tener un sistema híbrido en el cual el banco central podría ofrecer billeteras digitales para pagos de bajo valor, promoviendo la inclusión financiera a través de tecnologías de muy bajo costo para el manejo de dinero por parte de la ciudadanía, y un esquema de dos partes para pagos mayores.

El tema está aún en discusión y existen muchos temas que abordar antes que hayan masivamente CBDC en el mundo. El tema es complejo, pero potencialmente muy beneficioso para la ciudadanía, para aumentar la inclusión financiera, reducir los costos de transacción y proveer medios de pago seguro.

8. Comentarios finales

Bitcoin fue lanzado en 2009 para ser una moneda. No lo ha logrado y es improbable que lo haga. No hay antecedentes que en los países donde se les aceptó como moneda de curso legal, como El Salvador y otros por venir, haya precios que se fijen en Bitcoin, por lo tanto, no es unidad de cuenta. Su volatilidad de precios impide que se transformen en monedas de uso regular. Es altamente inconveniente poner precios en un activo con tanta volatilidad. En cambio, las *stablecoins* podrían contribuir a acelerar las transacciones transfronterizas y reducir los costos, algo que sería positivo en especial para las remesas de migrantes. Sin embargo, no son monedas, son certificados respaldados por monedas tradicionales y tienen los riesgos que al no ser reguladas no se puede proteger a los usuarios de fallas en el proveedor de la criptomoneda.

Un problema más complejo de los criptoactivos es su anonimato, lo que se presta para que sean vehículos de todo tipo de actividades delictuales y eso ciertamente reduce su beneficio social. Es posible algún grado de trazabilidad y determinar identidades en algunos de ellos, pero a costos y complejidades que hacen muy improbable que las agencias de seguridad puedan actuar oportunamente. Probablemente ponerlos bajo un esquema regulatorio que impida los negocios ilegales pueden ayudar a potenciar sus beneficios. La tecnología basada en criptografía con registro distribuidos y cadenas de bloque tiene muchas aplicaciones relevantes en finanzas, no como medios de pago, pero si en la creación, por ejemplo, de contratos inteligentes. En todo caso los tiempos de procesamiento y el consumo de energía son un problema no resuelto. En todo caso, existen otros algoritmos que permiten realizar validaciones más rápidas, aunque con menor grado de descentralización.

El problema de transacciones ilícitas se ha facilitado con las criptomonedas, pero ellas no son el origen ni su regulación la única solución. De hecho, muchos partidarios de las criptomonedas argumentan que una gran cantidad de delitos se financian en efectivo. Por

lo tanto, también hay que endurecer las restricciones al uso de efectivo en transacciones. Se deberían prohibir transacciones de alto valor en efectivo, como ya se hace en muchos países de Europa, y asimismo informar a las autoridades de todo depósito o retiro de efectivo por encima de algún límite razonablemente bajo.

La industria financiera está atravesando muchos cambios producto del uso de tecnologías. Aumenta la competencia y mejora le eficiencia, lo que contribuye a la inclusión financiera, pero aparecen nuevos riesgos. La protección del consumidor y los riesgos a la estabilidad financiera deben abordarse. Seguramente aparecerán muchos desarrollos nuevos y positivos, como será el uso de inteligencia artificial o uso de computadores más poderosos. Pero debe haber regulación que, protegiendo la integridad del sistema y, abriendo mayores espacios de competencia, mitigue sus riesgos.

Referencias

Adrian, Tobias y Tomsso Mancoini-Griffoli (2021), "Digital Forms of Money Could Be a Boon for Emerging Market and Lower-Income Economies if the Transition is Well Managed and Regulated", *Finance and Development*, IMF.

Auer, Rapahel y Raine Bhöme (2020), "The Technology of Retail Central Bank Digital Currency", BIS Quarterly Review, marzo.

Bank of England (2020), "Central Bank Digital Currency. Opportunities and Design", Discussion Paper, Future of Money.

BIS (2018), *Annual Report,* Bank of International Settlements.

BIS (2021), *Annual Report,* Bank of International Settlements.

BIS (2019), *Investigating the Impact of Global Stablecoins*, G7 Working Group on Stablecoins, Committee on Payments and Market Infraestructure.

Brunnermeir, Markus y Martin Oehmke (2013) "Bubbles, Financial Crises and Systemic Risk" en George M. Constantinides, Rene Stulz and Milton Harris (eds.), Handbook of the Economics of Finance, 2013, Vol. 2B, Chapter 18, pp. 1221-1288.

De Gregorio, José (2007), *Macroeconomía. Teoría y Políticas*, Pearson Educación.

Foley Sean, Jonathan R. Karlsen y Tālis J. Putniņš (2019), "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," *The Review of Financial Studies*, vol 32, no 5, pp 1798–853

Garber, Peter (1990), "Famous First Bubbles", *Journal of Economics Perspectives* 4(2): 35-54.

IOSCO (2017), *IOSCO Research Report on Financial Technologies (Fintech)*, International Organization of Securities Commissions.

Obstfeld, Maurice y Kenneth Rogoff (2021), "Revisiting Speculative Hyperinflations in Monetary Models", *Review of Economic Dynamics* 40: 1-11.

Paquet-Clouston, Masarah, Bernhard Haslhofer y Benoît Dupont (2019), "Ransomware Payments in the Bitcoin Ecosystem", *Journal of Cybersecurity*, Mayo, pp. 1–11.

Russo, Camila (2020), *The Infinite Machine. How an Army of Crypto Hackers is Building the Next Internet with Etherum*, Harper Business.

Tinn, Katrin y Christophe Dubach (2921), "Central Bank Digital Currency with Asymmetric Privacy", mimeo.

WEF (2021), "Decentralized Finance (DeFi) Policy-Maker Toolkit", White Paper, World Economic Forum in collaboration with the Wharton Blockchain and Digital Asset Project.