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

1. La operación de las criptomonedas

El dinero se basa en dos tipos de tecnologías (BIS, 2018). La más antigua es la de "fichas" *(tokens)*, que hoy corresponden a los billetes y monedas.

La otra tecnología son las "cuentas". En este caso, se verifica que haya dinero en la cuenta, y se evita el "doble gasto", es decir, que una cantidad de dinero se ocupe dos veces. Están centralizadas en los bancos, que registran las transacciones y las autorizan si hay fondos; y permiten trazar la historia de las transacciones y operaciones ilegales, aunque no siempre con éxito.

Las criptomonedas usan esta tecnología, son completamente trazables pero anónimas, lo que impide a las instituciones financieras cumplir con la regulación de *know your customer* (KYC).

Las cuentas se denominan "billeteras", accesibles con una clave pública, una expresión alfanumérica con la que son identificadas en la red, y una privada. No hay otro registro para identificar al (los/las) propietario(s). El anonimato es una característica fundamental de las criptomonedas, por lo que son el medio preferido para transacciones ilegales.

Para acceder a las billeteras, firmar y dar órdenes de pago, cada cuenta tiene una clave privada, generada a través de criptografía por la clave pública, conocida solo por su propietario. Su pérdida representa la pérdida de la billetera y su contenido.

Las transacciones se realizan dando órdenes de pago desde una billetera digital a otra, de forma directa entre dos individuos, o a través de una plataforma de transacciones de criptomonedas. La plataforma permite, además, realizar operaciones de cambio con monedas de curso legal.

La verificación de las transacciones en criptomonedas es descentralizada y segura. Se basa en un registro distribuido *(distributed ledger)* entre todos los participantes, donde se van validando y agregando todas las transacciones en forma secuencial. Cada nodo tiene toda la historia de las transacciones, guardada en muchos computadores, lo que, unido a las complejidades criptográficas, la hacen inviolable.

Supongamos que "A" va a transferir Bitcoin a "B". Desde su billetera digital, A da la orden de transferencia a la clave pública de B, la que se transmite a todos los nodos de la red, donde los mineros –operadores de los nodos- "excavan la orden" para resolver el problema criptográfico (conocido como "prueba de trabajo") de las transacciones aún no validadas. El primer minero que lo resuelve recibe un incentivo, 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 y permite ir agregando bloques, los que no se pueden modificar y constituyen los registros que se distribuyen en la red.

En Bitcoin, el premio al "minero" por resolver el problema criptográfico consiste en Bitcoins nuevos, los que han ido cayendo en el tiempo, pues el creador del sistema estableció un límite de 21 millones de Bitcoins, a fin de evitar su emisión ilimitada (debasing). En la actualidad, hay unos 19 millones de Bitcoins emitidos.

Una ventaja es que no hay costos de transacción relevantes. Sin embargo, una vez que se llegue a su máximo, los mineros cobrarán comisiones para mantener operando la minería.

2. Las criptomonedas: no son dinero, son activos

El dinero es definido por sus funciones, que son tres:

◦ *Es una unidad de cuenta:* los precios se fijan en dinero. Para que sea unidad de cuenta efectiva, es indispensable que tenga un valor estable, misión del Banco Central.

Las criptomonedas no han tenido estabilidad de precios. Por ejemplo, a principios de 2021, vender un inmueble en Chile en 5000 UF, equivalía a $ 145 millones. Al valor del Bitcoin y dólar al primero de enero, el precio en Bitcoin sería 7.07. Si el precio se diera en Bitcoin, para abril hubiera subido de $ 145 a $ 314 millones.

El valor tampoco es estable en las llamadas *stablecoins,* cuyo precio está atado a monedas regulares. Si el Bitcoin remplazara al dólar, el año 2018 la inflación hubiera sido de 270%, y el año 2020 habría tenido una deflación de 75%.

◦ *Es un medio de pago:* los bienes se intercambian por dinero, por lo que la estabilidad de precios es importante. Si se cierra un negocio y se paga después en dinero, no es mayor problema. En cambio, la volatilidad de los precios de las criptomonedas no las hace convenientes como medio de pago.

Uno podría hacer el pago en criptomonedas al valor del momento en que se realiza el intercambio, lo que es 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:* sirve para traspasar valor a través del tiempo, proveyendo un valor estable en el tiempo.

Las criptomonedas sirven para ahorrar, al igual que las acciones, bonos, o cualquier activo.

Tether, una stablecoin, se cambia uno a uno con el dólar. Evita la volatilidad, pero no es una moneda independiente, pues debe estar completamente respaldada por dólares; para emitir la criptomoneda hay que adquirir dólares, de manera que el activo subyacente es el dólar.

Tether es la tercera moneda digital, con una capitalización de US$ 63 mil millones. Facilitaría las transferencias de migrantes a sus países sin los costos actuales, pero fuera de cualquier regulación, control de flujos de capitales y protección al usuario.

En resumen, el objetivo por el cual el Bitcoin fue creado no se ha cumplido, no es una moneda. En 2019, solo el 1,3% de las transacciones de Bitcoin fueron con comercios, el resto, operaciones financieras.

Otro problema es el tiempo para validar las transacciones, en torno a 10 minutos. El sistema de Bitcoin puede procesar 7 transacciones por segundo, mientras Visa procesa 60.000.

Hay plataformas privadas muy rápidas 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 las transacciones por segundo, pero operan en plataformas privadas. Hay también tecnologías como *Lightning Network,* una segunda capa a la red de Bitcoin para pagos de bajo valor, que consiste en un canal privado, donde los clientes depositan bitcoins y hacen transacciones instantáneas, y cuando el canal se cierra empieza la prueba de trabajo. En abril de 2021, solo un 2% de los nodos de Bitcoin admitían la segunda capa.

3. 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. No obstante, las criptomonedas no tienen ningún activo subyacente ni valor intrínseco. En economía, a ese tipo de activos se les llama *burbujas.*

El dinero también es una burbuja, pues no tiene un valor intrínseco, y se valora porque se confía en que el resto de la economía lo acepta. Que tenga curso legal, garantizado por el estado, y los bancos centrales ajusten la oferta de manera creíble para que su valor sea estable, lo convierte en moneda.

¿Que sea una burbuja significa que su precio de largo plazo debiera ser cero? No necesariamente, si existe demanda por el activo. El Bitcoin y las criptomonedas podrían ser el "nuevo oro" (Tirole, 2017), que se demanda porque no está correlacionado con la inflación ni el ciclo económico mundial, pero tampoco se puede descartar que su valor vaya a cero.

¿Es irracional comprar Bitcoins? No. Puede ser una burbuja especulativa racional y tener un valor positivo y elevado, pero es imposible tener noción del valor al que podrá llegar.

4. Los riesgos y costos

4.1 Lavado de dinero y actividad delictual

Bitcoin es seguro, trazable y anónimo, pero esto último es su mayor riesgo desde el punto de vista social. El rapto de sistemas computacionales *(ransomware)* y otras actividades delictuales han envuelto el pago en criptomonedas, lo que hace, además, que no tengan fronteras, complejizando su rastreo.

La regulación KYC *(know your customer)* es importante para los sistemas financieros, pero no se puede asegurar en las operaciones en criptomonedas. Se argumenta que Bitcoin es pseudo-anónima. Una vez que entra en transacciones, toda su historia queda registrada, pero son muy pocas aquellas

para compra de bienes y servicios, y el cambio por monedas regulares puede realizarse en jurisdicciones que no compartan internacionalmente su información de actividades ilegales. Asimismo, ha aparecido una criptomoneda nueva, Monero, imposible de trazar.

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 fueron ilegales, cercano a la escala del mercado de drogas en Estados Unidos y Europa.

Otro problema es la evasión de impuestos, alentada por el anonimato, y los riesgos operacionales y exposición a fraudes.

4.2 Uso de energía

La actividad minera de criptomonedas es muy intensiva en energía. Se necesitan grandes servidores para resolver los problemas criptográficos para las pruebas de trabajo.

El Centro Cambridge de Finanzas Alternativas estima que Bitcoin consume 130 Terawatt hora por año, mayor al consumo

de Suecia o Noruega. Se ha argumentado que usa menos energía que la industria bancaria, pero lo relevante debería ser el consumo por unidad de valor agregado, y si el Bitcoin es un activo financiero sin valor intrínseco, su valor agregado sería muy bajo.

Actualmente se está trabajando en la tecnología de prueba de participación *(proof of stake),* que ahorra energía, la que selecciona a los nodos que validan las transacciones basado en su participación en el valor total de la criptomoneda.

4.3 Controles de capital

Un tema muy discutido en economías emergentes es el uso de controles de capital para regular sus entradas y salidas, cuestión que no es posible con las criptomonedas. Si alguien quiere sacar capitales de una economía, puede usar moneda local para comprar criptomonedas y venderlas en el país de destino, o cambiarlas fuera de las fronteras, y no queda registro de la transacción transfronteriza.

5. 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 *(FinTech)* es tal vez el mayor cambio financiero en décadas. Ha sido disruptivo y abre un abanico de oportunidades y riesgos.

Las cadenas de bloques pueden usarse en muchas aplicaciones con seguridad y eficiencia, como registrar el catastro de propiedades, la información médica, y muchas otras.

Mención especial merece Ethereum -cuya moneda digital es Ether-, la segunda en capitalización después de Bitcoin. Es una plataforma para crear aplicaciones con la tecnología de cadenas de bloques que, una vez validadas, no se pueden eliminar ni cambiar. La más conocida es la de *contratos inteligentes (smart contracts),* que especifican condiciones y dan curso a los pagos u otras acciones automáticas cuando aquéllas se cumplen. Es una tecnología nueva pero con mucho potencial, puede reducir costos de intermediación y fraude, y es muy segura. Se usa también para levantar fondos que financien inversiones, emitiendo como respaldo una moneda en un ICO *(initial coin offering).* Hay problemas de fe pública y protección del consumidor, por eso las emisiones de acciones son muy reguladas.

La industria financiera está atravesando muchos cambios producto del uso de tecnologías. Aumenta la competencia y mejora la eficiencia, lo que contribuye a la inclusión financiera, pero aparecen nuevos riesgos.

Esto es parte de una tendencia mayor llamada DeFi *(decentralized finance),* que usa las tecnologías de registros distribuidos y cadenas de bloques, replicando las funciones de los sistemas financieros, pero de manera descentralizada y digital. Esta revolución digital en finanzas tiene muchas posibilidades de mejorar la inclusión financiera, proveyendo servicios simples y a bajo costo. Sin embargo, hay muchos temas regulatorios pendientes, como la protección del consumidor y de datos personales, la continuidad operacional y los riesgos financieros.

6. Las monedas digitales de los bancos centrales

La mayoría de los bancos centrales están en la "prueba de concepto" respecto de criptomonedas, y todos estudian las posibilidades de implementación.

Es necesario que las autoridades monetarias y financieras tengan conocimiento de las tecnologías y su aplicación para el bienestar de la población, pero también que monitoreen sus

implicancias para la regulación y la estabilidad financiera. La existencia de criptomonedas privadas podría generar problemas de flujos transfronterizos y volatilidad de los tipos de cambio que requieren atención. Asimismo, nada asegura que las *stablecoins* tengan el suficiente respaldo de sus monedas. Si las plataformas de monedas digitales son *hackeadas,* nadie es responsable.

Pero también las nuevas tecnologías podrían beneficiar a la ciudadanía con un sistema de pagos simple, seguro y eficiente. Las monedas de los bancos centrales, conocidas como CBDC *(central bank digital currency),* podrían avanzar en inclusión financiera.

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 vía *blockchain,* y billeteras digitales para mantener el dinero. Sin embargo, esto podría crear desintermediación con el sistema bancario y su función de transformación de madurez y otorgamiento de crédito, con consecuencias negativas sobre la economía. El banco central no puede dedicarse a hacer préstamos e incurrir en riesgo de crédito. Otra pregunta relevante es quiénes tendrán acceso al banco central como prestamista de última instancia.

No es necesario que las CBDC sean completamente descentralizadas. Se podrían usar plataformas privadas donde hay validadores autorizados, podría ser el banco central el único validador, o se pueden usar algoritmos rápidos como la *proof of authority,* donde hay solo algunos nodos autorizados a validar.

Un desarrollo en sus primeras etapas que podría resolver la dificultad de violación de la privacidad de las CBDC son los modelos de privacidad asimétrica (Tinn and Dubach, 2021), donde las personas tendrían dos billeteras, una anónima y otra con identificación. Las transferencias llegarían a la billetera no anónima, pero los traspasos se podrían hacer desde cualquiera de las dos, pues para impuestos y regulación, lo más relevante es identificar al receptor.

Las CBDC podrían constituirse como un sistema de dos partes que mantenga la forma actual de distribución de dinero. El banco central emite CBDC solo a entidades financieras reguladas, y éstas ofrecen billeteras digitales a sus clientes (Bank of England, 2020). O podría ser un sistema híbrido en el cual el banco central ofrezca billeteras digitales para pagos de bajo valor, promoviendo la inclusión financiera a través de tecnologías de bajo costo para el manejo de dinero, y un esquema de dos partes para pagos mayores.

7. 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, 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 positivo, en especial para las remesas de migrantes. Sin embargo, no son monedas, son certificados respaldados por monedas tradicionales y, 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 las presta como vehículos de actividades delictuales. Es posible algún grado de trazabilidad y determinar identidades, pero a costos y complejidades que hacen muy

improbable actuar oportunamente. Probablemente, ponerlas bajo un esquema regulatorio que impida los negocios ilegales puede ayudar a potenciar sus beneficios. La tecnología basada en criptografía con registro distribuido y cadenas de bloque tiene muchas aplicaciones relevantes en finanzas, no como medios de pago, pero sí en la creación, por ejemplo, de contratos inteligentes, pero los tiempos de procesamiento y el consumo de energía son un problema. 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 la única solución es su regulación. Muchos partidarios de las criptomonedas argumentan que una gran cantidad de delitos se financian en efectivo, por lo que también hay que endurecer las restricciones al uso de efectivo en transacciones.

La industria financiera está atravesando muchos cambios producto del uso de tecnologías. Aumenta la competencia y mejora la 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 de computadores más poderosos. Pero debe haber regulación que, protegiendo la integridad del sistema y abriendo mayores espacios de competencia, mitigue sus riesgos.

José De Gregorio*
Decano Facultad de Economía y Negocios
Universidad de Chile

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.

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