

CUADERNOS CEF / N°2

Criptomonedas, Aplicaciones Potenciales de Blockchain y Desafíos Regulatorios

HÉCTOR ACUÑA



Universidad de los Andes

CEF - Centro Estudios Financieros

NOVIEMBRE | 2018

Criptomonedas, Aplicaciones Potenciales de Blockchain y Desafíos Regulatorios

HÉCTOR ACUÑA¹

Resumen

La tecnología blockchain posibilita iniciativas que crean nuevas oportunidades para un mundo más próspero. Prosperidad, por encima de todo, significa elevar el nivel de calidad de vida. Para ello, la gente necesita disponer de medios, herramientas y oportunidades para crear riqueza material y crecer económicamente. Pero también incluye más cosas: seguridad personal, salud, educación, sostenibilidad medioambiental, oportunidades para construir y controlar nuestro destino y participar en la economía y en la sociedad. Para prosperar, un individuo necesita tener, como mínimo, acceso a alguna forma de servicio financiero básico que le permita acumular y mover valor con seguridad, capacidad de comunicación, herramientas transaccionales con las que conectarse a la economía global, seguridad, protección y garantía del derecho a la tierra y a otros bienes que posea legalmente.

Hasta el momento, esta tecnología aplicada a criptomonedas 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.

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.

¹ Investigador del Centro de Estudios Financieros - ESE Business School de la Universidad de Los Andes. Agradezco los valiosos comentarios de M. Cecilia Cifuentes. Cualquier error u omisión es de mi exclusiva responsabilidad. Email: hacuna.es@uandes.cl.

Contenido

1. ¿Es la Tecnología Blockchain una Revolución Modernizadora en Marcha?.....	4
1.1 Blockchain y confianza.....	5
1.1.1 El control del doble gasto y del riesgo de corridas bancarias.....	6
1.1.2 Automatización y desintermediación eficaz.....	7
1.1.3 El rol de los contratos inteligentes.....	8
1.1.4 Oferta Inicial de Monedas (ICO).....	9
1.2 Los Estados y la tecnología blockchain.....	9
1.2.1 La tecnología blockchain en América Latina.....	10
2. ¿Tienen las criptomonedas los atributos necesarios para reemplazar al dinero actual? Posición del Banco de Pagos Internacionales - Reporte Económico Anual 2018.....	11
2.1 Rol del dinero y funcionamiento de los actuales sistemas monetario y de pagos.....	13
2.2 Criptomonedas y la promesa de confianza descentralizada.....	14
2.2.1 Tecnología de contabilidad distribuida en criptomonedas.....	15
2.3 Análisis de las limitaciones económicas de las criptomonedas descentralizadas.....	20
2.4 Otros usos potenciales de la tecnología de registro distribuido.....	23
2.5 Desafíos para las políticas económicas.....	23
2.5.1 Desafíos regulatorios ante las criptomonedas.....	24
2.6 ¿Deberían emitir los bancos centrales sus propias monedas digitales?.....	26
3. Más Allá de las Criptomonedas: Aplicaciones de Tecnología Blockchain.....	27
3.1 Contratos inteligentes.....	27
3.1.1 Gestión de la ayuda humanitaria.....	28
3.2 Estonia, país digital.....	28
3.3 Ofertas Iniciales de Monedas (ICOs).....	29
3.3.1 Diferencias entre ICO e IPO.....	30
3.3.2 Beneficios potenciales de las ICOs.....	31
3.3.3 Regulación de ICOs en el mundo.....	31
3.3.3.1 Regulación en Suiza.....	32
3.3.4 Futuro de las ICOs.....	35
4. Blockchain dentro del Marco de la Irrupción de FinTech: Desafíos para la Banca Central.....	36
4.1 Rol de los bancos centrales.....	37
4.2 Oportunidades que entrega FinTech: Contribuciones, riesgos potenciales y desafíos.....	38
4.3 Impacto potencial de las tecnologías de contabilidad distribuida y de cadena de bloques (blockchain).....	41
4.4 Bancos centrales y la posibilidad de crear sus propias monedas digitales.....	42
4.5 Dilemas y desafíos para los banqueros centrales y reguladores.....	43
4.6 FinTech en América Latina.....	45
4.6.1 Regulación de FinTech en el sistema financiero chileno.....	45
5. Conclusiones y Discusión.....	47

1. ¿Es la Tecnología Blockchain una Revolución Modernizadora en Marcha?

La era digital nos ha acostumbrado a procesos continuos de cambio, los que son cada vez más rápidos y profundos. Un ejemplo es el impacto en nuestra vida de los smartphones, que han alterado en un cortísimo período la forma tradicional de hacer muchas cosas. Llama entonces la atención que, en este contexto específico donde el cambio y la transformación pasan a ser la norma, tantos expertos y organismos internacionales hablen con tanta insistencia del carácter revolucionario y profundamente transformador de la tecnología blockchain². Lo explicamos a continuación.

Si pedimos nuestra primera tarjeta de crédito o solicitamos un préstamo, lo primero que el banco valorará será cuánto crédito tenemos, nuestra “calificación crediticia”. Esta cifra representa nuestra solvencia y, en consecuencia, el riesgo de que no cumplamos. Es el resultado de una serie de factores, que van desde el plazo de amortización del préstamo al historial de pagos. La mayoría de los préstamos minoristas dependen de esto. Pero este cálculo tiene muchas falencias.

En primer lugar, es muy reductivo. Pensemos en el propietario de un pequeño negocio que quiere pedir un préstamo. Lo más frecuente es que el encargado de turno del banco base su decisión en la documentación que aporta la persona, su identidad considerada desde un solo punto de vista y su calificación crediticia. Por supuesto, una persona es mucho más que la suma de su número de la seguridad social, su lugar de nacimiento, su domicilio y su historial de crédito. Pero el banco no sabe, ni le importa, si somos unos empleados cumplidores, unos voluntarios activos, unos ciudadanos comprometidos, o los entrenadores del equipo de fútbol de nuestro hijo. El encargado de conceder el préstamo puede valorar que nos comportemos con integridad, pero el sistema de calificación del banco no. Estos componentes de la reputación son difíciles de formular, documentar y usar tal y como están concebidos los sistemas social y económico actuales.

Luego, ¿qué reputación tenemos? Todos tenemos al menos una. La reputación es un factor esencial de la confianza en los negocios y en la vida cotidiana. Hasta ahora, los intermediarios financieros no han usado la reputación como base para crear confianza entre individuos y bancos. Entonces, ¿qué hacen los miles de millones de personas que no tienen reputación más allá de su círculo social inmediato? Muchas personas, generalmente las de menores ingresos, no pueden cumplir con los requisitos de identidad exigidos, como presentar un documento de identidad, un certificado de residencia o un historial financiero. Por lo tanto, no tienen la posibilidad de acceder a servicios financieros formales.

² Para un análisis profundo sobre cómo funciona la tecnología blockchain, ver Acuña (2017), disponible en: <https://www.esec.cl/esec/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html>

El sistema blockchain puede resolver este problema dando a las personas la posibilidad de crear identidades únicas con varios atributos, entre ellos el historial de transacciones, y así, dar un acceso alternativo al mercado de capitales y al financiamiento, paralelo al que brinda el sistema bancario tradicional. Por lo tanto, blockchain permite distribuir mejor las oportunidades en vez de redistribuir riqueza, ya que permite que las personas tengan una identidad y una reputación única y verificable, y puedan compartirla en el nivel y con las personas que deseen.

Sigue habiendo muchos casos —sobre todo en materia de crédito— en los que el sistema blockchain crea confianza entre las partes cuando esa confianza se necesita. La tecnología blockchain no sólo funciona para que el capital prestado vaya al prestatario, sino que también garantiza que éste lo devuelva con intereses. Da poder a las dos partes con sus propios datos, refuerza su privacidad y genera una nueva identidad económica perdurable basada en factores como el historial económico y el capital social de cada cual. Como esta tecnología registra y archiva todas las transacciones en un registro inmutable, todas ellas pueden servir para incrementar nuestra reputación y solvencia.

Un sistema basado en la reputación baja los costos para los buenos actores y los sube para los malos, lo que se transforma en el mejor incentivo. En sistemas basados en la reputación, nuestra solvencia derivará de un conjunto de atributos que forman nuestra identidad y avalan nuestra capacidad de devolver un préstamo. La calificación crediticia de las empresas también cambiará para incluir la nueva información y los nuevos factores que el sistema blockchain hace posibles.

Imaginemos herramientas que integren la reputación y rastreen diferentes aspectos de ella, como la solvencia económica, la competencia profesional y la conciencia social. Imaginemos una forma de préstamo basada en valores compartidos, en la que la gente que nos presta dinero valora el papel que desempeñamos en la comunidad y nuestras metas. A modo de introducción, en este capítulo resumiremos el trabajo de Bravo y Hardings (2018) enfocándonos precisamente en las características de esta tecnología que la hacen revolucionaria y transformadora.

1.1 Blockchain y confianza

La aparición de blockchain como base de funcionamiento de la criptomoneda Bitcoin en 2008 es disruptiva ya que no se requiere una entidad central en la que todos los participantes deban confiar. De hecho, los participantes que hacen funcionar el sistema tampoco requieren confianza mutua, ni siquiera es necesario que se conozcan entre ellos. Es más, se asume y tolera el hecho de que exista un número relevante de agentes maliciosos. Esto constituye lo que se conoce como sistema de confianza cero.

Se suele afirmar que la confianza es una condición necesaria para el buen funcionamiento de cualquier colectividad, sea ésta un sistema político, un mercado, una empresa o cualquier otra. Además, hoy en día se hace el diagnóstico de que estas confianzas tan necesarias se encuentran en crisis, y que *“recuperarlas parece una misión tan urgente como poco realista”*.

Es por este motivo que la irrupción de blockchain es tan significativa. Esta tecnología es capaz de enfrentar y superar dicha crisis de un modo radical y de efecto instantáneo: haciendo innecesaria la confianza. Para ser más precisos, depositándola en otra parte, dejando de confiar en las personas e instituciones para hacerlo en el método con el que se interactúa con ellas.

Así también, *“blockchain ofrece una nueva forma de lidiar con la incertidumbre del futuro al entregar la posibilidad de hacer acuerdos incensurables, irrefutables, inmodificables y autoejecutables (por lo que no requieren la voluntad de un sujeto obligado a cumplir su compromiso en el futuro), extendiendo así el carácter de sistema de confianza cero a la coordinación de acciones presentes y futuras entre distintos agentes”*.

La confianza deja así de ser una condición y pasa a ser el resultado de una interacción exitosa. No sorprende entonces que blockchain sea el entorno adecuado para el desarrollo de economías y modelos de negocio colaborativos.

Tenemos además que en este ecosistema cualquier participante puede agregar transacciones con nueva información que se añade a la ya existente, siempre y cuando siga las reglas acordadas para que una transacción sea válida. Una regla inherente al blockchain es que no se puede modificar información anterior; solamente agregar información nueva. Para hacer posible un ecosistema en que no sólo no se requiera, sino que no sea posible que exista un ente central controlando el proceso, también es necesario manejar descentralizadamente todo lo relacionado con la operación. Esto incluye la lógica mediante la cual un participante se incorpora o sale de la red, la forma en la que se actualizan las reglas mediante las cuales se determina que una transacción es válida y la forma en la cual se regula la velocidad a la que se incorpora nueva información a esta base de datos compartida y distribuida.

1.1.1 El control del doble gasto y del riesgo de corridas bancarias

Si se pudiese garantizar que sólo el titular pudiese disponer de lo propio y que sólo pudiese enajenarlo una única vez, es decir, si se pudiese evitar el doble gasto, la realización de fraudes sería imposible. La solución dada hasta ahora para evitar el doble gasto fue la tradicional intermediación de agentes de confianza, es decir, la existencia de un tercero quien centraliza y administra la información, y cuyos registros son los que establecen quién tiene qué o cuánto, siendo él quien pone las reglas para su modificación.

Pero en algún momento, los banqueros se dieron cuenta de que no era necesario mantener en custodia todo lo depositado; que bastaba con tener en caja lo suficiente para pagar a quienes fueran a retirar sus fondos, lo que suele ocurrir en forma diferida y parcial. Esto permitía volver a prestar el resto del dinero no una, sino varias veces más. Nace así el sistema de banca fraccional o de encaje, que predomina hasta hoy, con sus virtudes y riesgos. Implica la aceptación del doble gasto, pero sólo cuando quien lo ejecuta es el agente o intermediario de confianza mutua. En rigor no es doble, sino que por factores bastante mayores a dos (de seis, diez y hasta veinte veces). En la otra arista, implica también el riesgo de corrida bancaria, que consiste en la sincronización de los depositantes solicitando la devolución de lo suyo, y que se vuelve un requerimiento imposible de satisfacer por el banquero que así opera, salvo una operación de rescate por parte del Estado.

En este modelo de banca fraccional o de encaje, el riesgo de corridas bancarias es inherente, por lo que su operación arrastra un compromiso inevitable de la fe pública. Es esta característica la que justifica y motiva buena parte de la regulación bancaria estatal, incluyendo la concesión de la exclusividad del giro bancario a los tenedores de licencias estatales.

En blockchain, la titularidad de lo transado se reduce a la tenencia de la llave (o clave) privada³, traspasando así la responsabilidad de su cuidado y buen uso a quien la generó. Por su parte, la imposibilidad de disponer dos veces de algo no puede estar más garantizada, ya que la consistencia histórica de los registros es la fuente de validación de las transacciones en el sistema.

De esta forma, la tecnología blockchain posibilita un control eficaz del doble gasto. Así, se hace innecesaria la intermediación de agentes de confianza y por ende, no es necesaria la aceptación del doble gasto del agente de confianza, reduciendo a cero el riesgo de corrida bancaria y eliminando la necesidad de regulación bancaria estatal en esta materia.

1.1.2 Automatización y desintermediación eficaz

Uno de los grandes objetivos perseguidos por los creadores de la tecnología blockchain era lograr la desintermediación en el intercambio económico. Es más, el objetivo explícito de Bitcoin, y primer caso de uso de esta tecnología, fue la desintermediación en la transferencia, particularmente la internacional, de valores.

Por muy política que haya sido la motivación inicial, el resultado es esencialmente económico, puesto que, aunque estamos acostumbrados a ella -al punto de dejar de observarla-, toda intermediación implica fricción en la economía, disminución en la velocidad de circulación del dinero y encarecimiento del servicio intermediado. En el caso

³ Para más detalle, ver Acuña (2017), capítulo 6, disponible en: <https://www.ese.cl/ese/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html>

de una transferencia internacional de dinero intervienen más de una decena de agentes de confianza sobre algún aspecto de la operación, tarda entre 3 y 5 días, y tiene asociado un cargo mínimo de entre cuarenta y cien dólares⁴. En contraste, la transferencia de criptoactivos de una billetera a otra tarda minutos y no tiene intermediarios ni, en principio, costo alguno asociado, independientemente de dónde se encuentre su titular. Se trata de otro orden de eficiencia, imposible de alcanzar por los que hacen de la intermediación su negocio.

1.1.3 El rol de los contratos inteligentes

Otra aplicación disruptiva de la tecnología blockchain es la construcción de contratos inteligentes que vienen a sustituir las instrucciones notariales.

En nuestro sistema se presentan con frecuencia saltos de confianza difíciles de resolver entre las partes. *“Piénsese, por ejemplo, en la compraventa de un inmueble, donde el comprador sólo está dispuesto a pagar por él una vez que esté inscrito a su nombre en el registro del Conservador de Bienes Raíces, mientras que el vendedor sólo está dispuesto a inscribirlo cuando haya recibido el pago. Ese dilema se resuelve habitualmente acudiendo a alguien que dé confianza a los dos (un notario) a quien le entregan el monto comprometido para que se lo entregue al vendedor cuando demuestre haber hecho la inscripción”*.

En la actualidad, y por medio de la tecnología blockchain, es posible sustituir al notario por un contrato inteligente, incorporando una regla o condición sencilla (el cumplimiento de un plazo o constatar una anotación, como en el ejemplo), pero también la articulación de todo un modelo de negocios, infinitamente complejo.

Como resultado tenemos que es posible reemplazar complejas estructuras empresariales o sistemas completos por un simple código, llevando así la desintermediación a otro nivel. Se trata además de un código alojado en el blockchain, por lo que su integridad y estabilidad están garantizadas, y se auto ejecuta. Combinando estos elementos, se encuentra que blockchain lleva también la automatización a otro nivel. Así, por ejemplo, es posible lograr la *“desintermediación automatizada del crédito privado (social lending P2P), que anula el spread, en beneficio de los intervinientes; al igual que es posible la automatización de sistemas de seguros donde el costo de la prima es finalmente idéntico a la distribución del costo del total de siniestros entre todos los asegurados (con o sin factores de corrección), sin recargo ni necesidad de compañía aseguradora tradicional alguna”*.

En el capítulo 3 abordaremos en profundidad el abanico de posibilidades que ofrece la tecnología blockchain aplicada a contratos inteligentes en diversas áreas e industrias.

⁴ Bravo y Hardings (2018), pág. 23. D. Kennedy de Scotiabank, en su exposición en el Blockchain Summit Latam Chile 2018, indicó que una transferencia desde Canadá a Chile cuesta 90 dólares, independiente del monto a transferir, lo cual hace inviable el envío de montos pequeños. En otros trabajos, y en el caso de montos de transferencia pequeños, se mencionan tarifas cercanas al 9-10% del monto a transferir.

1.1.4 Oferta Inicial de Monedas (ICO)

El paradigma de desintermediarlo todo en beneficio de los agentes finales, propio de blockchain, también se puede aplicar a la organización de una empresa.

La posibilidad que otorga un sistema de confianza cero como blockchain de interactuar fácilmente y de modo seguro con grandes universos de sujetos distribuidos por el mundo, combinados con la ductilidad y certeza que aportan los contratos inteligentes, ha permitido no sólo articular eficientes mecanismos de financiamiento colectivo o *crowdfunding*, sino también redefinir el rol que puede desempeñar el capital en una organización productiva.

Con blockchain, es posible financiar un proyecto o desarrollo no mediante el financiamiento de un socio capitalista, sino mediante la venta anticipada de los servicios que aún no existen pero que se espera que existan tras el desarrollo del proyecto. Estas expectativas de servicio se *tokenizan* (es decir, se monetizan digitalmente) y se ofrecen con la expectativa de venderlas en un monto y cantidad suficiente para financiar los procesos de un proyecto. Estos criptoactivos son, como todo *token*, libremente transables, lo que permite la especulación respecto a su valor.

Además de recaudar financiamiento, el modelo garantiza tracción de uso de la solución o servicio apenas esté disponible, así como una masa crítica de usuarios que active las externalidades de red, lo que mejora el pronóstico de éxito del proyecto. De este modo, se puede perfectamente articular una empresa que absorbe significativos costos de desarrollo sin necesidad de requerir un gran capital que demande renta. En el capítulo 3 analizaremos en mayor detalle este modelo de financiamiento.

1.2 Los Estados y la tecnología blockchain

Como hemos visto, las reglas bajo las que opera la tecnología blockchain cuestionan o desafían el monopolio del Estado como la fuente de legitimidad normativa, ignorando, por ejemplo, los silos jurisdiccionales. Esto *“se trata de una realidad desconcertante para los estados, pero que exige ser asumida e internalizada con prontitud. Entre otras cosas, porque también es fuente de poderosos nuevos recursos para la gestión pública”*.

1.2.1 La tecnología blockchain en América Latina

La irrupción de esta tecnología implica enormes oportunidades para la región de América Latina. La primera es que, a diferencia de otros ámbitos tecnológicos, no hay ningún impedimento para asumir el desafío desde nuestra región, ya que las lógicas de la tecnología blockchain se han traspasado a la comunidad que la construye. Así, tenemos que su desarrollo también se ha efectuado de un modo distribuido y descentralizado, lo que implica que *“no hay un gran centro en el cual todo suceda, al punto que signifique una desventaja no estar ahí, como ha sido la constante del desarrollo de otras tecnologías”*; y que no abundan las lógicas de captura, ni respecto a los avances logrados ni respecto a los conocimientos que los permitieron. No sólo hay acceso a los códigos, sino también hay libre acceso a recursos de aprendizaje de altísimo nivel y en continua evolución.

Por otra parte, se trata de una tecnología que no requiere de grandes inversiones en equipamiento o instalaciones. Sólo se requiere capacitación, esfuerzo humano y grandes cuotas de decisión. Por esta razón, los costos de desarrollo son comparativamente bajos y abordables por cualquiera de los estados de América Latina.

Adicionalmente, es posible observar que las fortalezas técnicas del blockchain calzan con fragilidades o amenazas que se ciernen sobre varios estados de la región, como son la corrupción, la fragilidad de la fiscalización y la dificultad para recaudar impuestos. *“Sólo piénsese en el impacto de los registros inmutables en la trazabilidad del gasto público o en los sistemas registrales, o en la posibilidad de autoejecución y autofiscalización normativa que implica el uso de smartcontracts obligatorios en, por ejemplo, procesos automatizados de mercados regulados”*.

Por su parte, el interés en la tecnología y sus alcances se ha despertado poco a poco, apareciendo cada vez con más frecuencia actividades de estudio y difusión, y pequeños casos de uso.

Se debe considerar que nos encontramos frente a una tecnología que *“altera capas profundas del entendimiento común, y que tiene –por ende– un enorme potencial transformador”*. Además, nada impide que quienes vayan a reconfigurar la realidad futura con el uso pleno de los nuevos recursos que aporta la tecnología blockchain provengan también de nuestra región, *“haciendo avanzar el proceso atendiendo las necesidades actuales de nuestros pueblos, nuestras economías y nuestros gobiernos”*.

2. ¿Tienen las criptomonedas⁵ los atributos necesarios para reemplazar al dinero actual? Posición del Banco de Pagos Internacionales - Reporte Económico Anual 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 (en adelante, 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 resolver⁶. A continuación, resumiremos esta sección del reporte del BIS, no sin antes dar una breve reseña sobre qué es el BIS y cuál es su labor.

El BIS es una organización internacional financiera propiedad de numerosos bancos centrales. Éste 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 (en adelante, DLT por su sigla en inglés).

⁵ Una criptomoneda es una divisa digital o virtual que utiliza criptografía para efectos de seguridad. Una de sus características principales, y probablemente la más atractiva, es su carácter orgánico, lo que la vuelve "inmune" a la interferencia o manipulación por parte de las autoridades. Las criptomonedas privadas, por definición, no son creadas por las autoridades.

⁶ 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 (por el señoreaje, que es la diferencia entre los costos de fabricación y el valor nominal de la moneda). Aun así, consideramos de gran interés conocer la posición de esta organización, y sus respectivos fundamentos, sobre las criptomonedas y su tecnología.

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.

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 energético⁷. 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.

⁷ Algunos expertos en informática sostienen que el problema del costo medioambiental y energético tendrías una solución factible con el uso de la computación cuántica. Por otra parte, el importante gasto energético solo se asocia a las cadenas de bloques que funcionan en base a la prueba de trabajo.

Algunas “cadenas alternativas” (altchains) han explorado otros algoritmos de consenso alternativos como la prueba de participación para hacer segura la red y que a la vez siga siendo descentralizada. No olvidemos que el objeto de los algoritmos de consenso es distribuir el derecho de decidir el estado de la blockchain entre un conjunto descentralizado de usuarios. Hay tres clases de usuarios seguros y descentralizados, y a cada grupo le corresponde un conjunto de algoritmos de consenso: los dueños de capacidad procesadora, que usan el algoritmo de prueba de trabajo normal; los participantes, que usan varios algoritmos de prueba de participación o actividad, y los miembros de una red social, que usan un algoritmo de consenso de tipo «federado», en el que un grupo autorizado de usuarios alcanza un consenso sobre el estado de la blockchain. Una cuarta forma de resolver el problema del gasto de energía, y es la que él llama “prueba de disco”, en la cual los dueños de espacio de almacenamiento en disco —gente que dedica parte de la memoria de su ordenador a mantener una red y desempeñar funciones reticulares— constituyen el grupo económico de usuarios.

2.1 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 más complejas y la actividad económica se expandió. Éste tiene tres 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.

Por otro lado, 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 realizados⁸.

⁸ 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

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 (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.

2.2 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.

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.

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.

2.2.1 Tecnología de contabilidad distribuida⁹ 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.

⁹ La contabilidad distribuida consiste en una base de datos compartida y actualizada por una red de usuarios. A diferencia de “la nube”, que es una base de datos con muchos usuarios, pero con una sola copia, manejada por una autoridad central o usuario principal, la contabilidad distribuida puede ser manejada y actualizada por varios de sus miembros, característica que la hace más segura ante los ciberataques, las caídas de los sistemas tecnológicos de información y otras fallas operacionales. La cadena de bloques es un tipo específico de contabilidad distribuida que incluye la historia encriptada de todas las transacciones (bloques) pasadas en cada registro actualizado. En resumen, la tecnología de contabilidad distribuida es una base de datos consensualmente compartida y sincronizada en una red distribuida en múltiples sitios, instituciones o lugares geográficos. Esto permite que las transacciones tengan “testigos” públicos. Cada usuario de la red puede acceder a los registros compartidos en esa red y puede disponer de una copia idéntica de ellos. Cualquier cambio o añadidura al sistema de contabilidad se refleja y copia en los registros de todos los participantes en cuestión de segundos o minutos. Para más detalle, ver Acuña (2017), disponible en: <https://www.esec.cl/esec/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html>

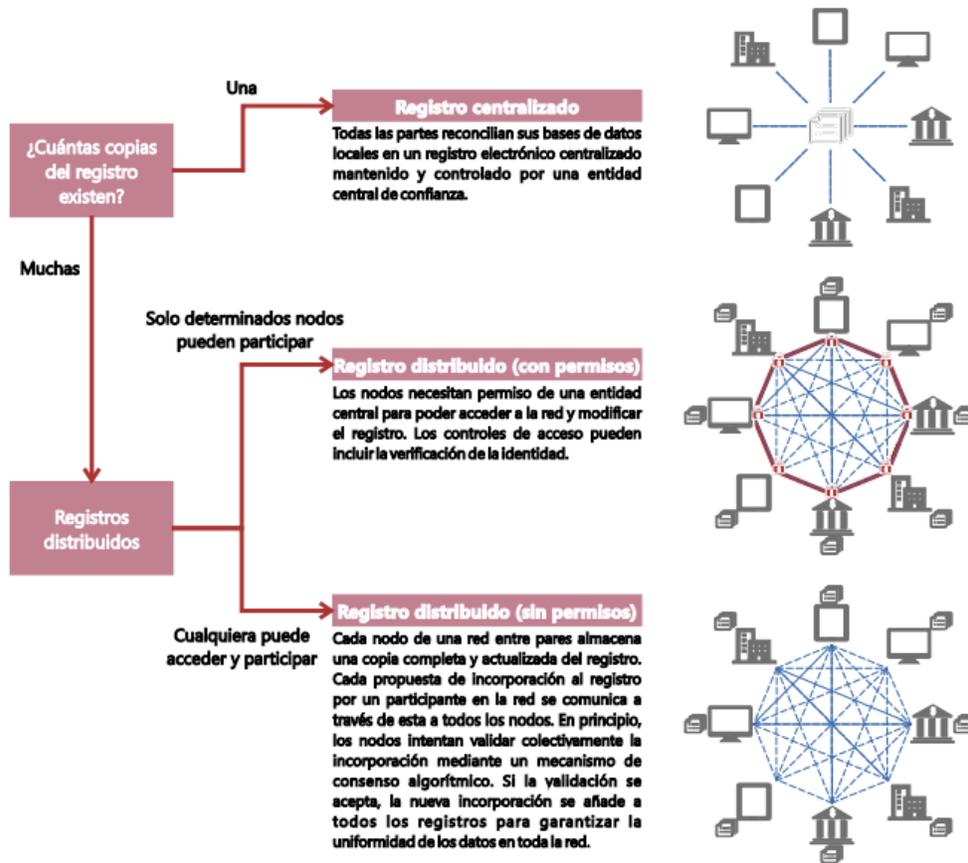
Cada usuario de la red almacena una copia actualizada de todo el libro (esto es lo que lo hace distribuido). Con un libro mayor distribuido, el intercambio de dinero digital entre pares es factible, ya que cada usuario puede verificar directamente en su copia del libro contable si se realizó una transferencia 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 1: Registro centralizado y registro descentralizado con y sin permisos

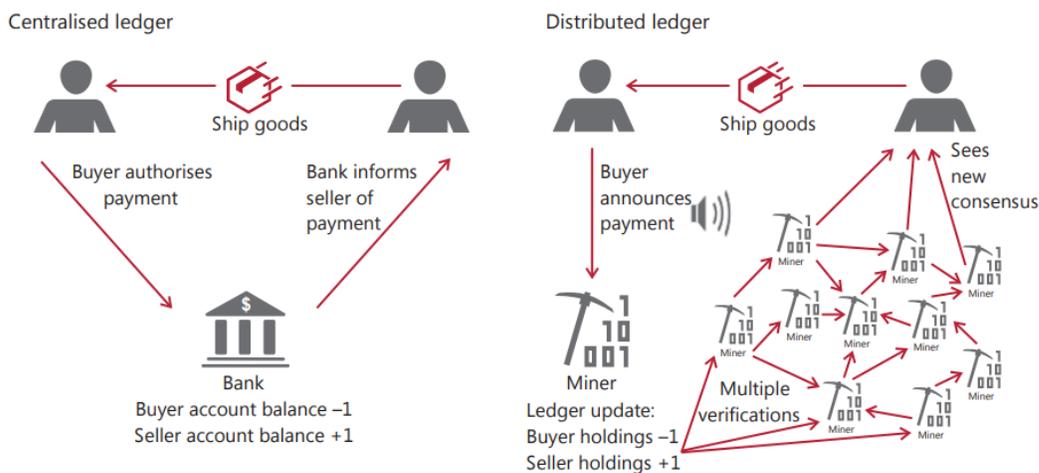


	Dinero electrónico privado basado en un sistema fiduciario	Criptomonedas de emisores privados	
		Con permisos	Sin permisos
1 Almacenamiento de saldos/posiciones	Registro (cuentas) almacenado de forma centralizada por bancos y otras instituciones financieras	Almacenamiento descentralizado del registro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

Fuente: Traducido de Natarajan et al. (2017), "Distributed Ledger Technology (DLT) and Blockchain", Grupo del Banco Mundial, FinTech Note, n° 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 2).

Figura 2: 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 denominado 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 trabajo¹⁰”, 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 reciben 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 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.

¹⁰ Para más detalles, ver Acuña (2017), disponible en: <https://www.ese.cl/ese/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html>

2.3 Análisis de las limitaciones económicas de las criptomonedas descentralizadas

De acuerdo con lo analizado en este capítulo, 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 terabyte¹¹.

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 generan estabilidad.

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

¹¹ Equivalente a 1.000 Gb.

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 probabilística¹².

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.

¹² 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.

2.4 Otros usos potenciales de la tecnología de registro distribuido

Aunque las criptomonedas no funcionan bien como dinero, la tecnología subyacente sí parece prometedora para otros ámbitos. Un ejemplo notable es el de los servicios de pagos transfronterizos de pequeña cuantía.

En términos más generales, si se compara con las soluciones tecnológicas centralizadas más comunes, 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 Alimentos¹³, 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 pagos¹⁴. 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.

2.5 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”.

¹³ 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.

¹⁴ Se analiza en detalle en el capítulo 3.

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.

2.5.1 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*¹⁵. 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 generará 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.

¹⁵ Se analizan en detalle en el capítulo 3.

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 ICOs 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 ICOs 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 ICOs 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.

2.6 ¿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 (en adelante 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.

3. Más Allá de las Criptomonedas: Aplicaciones de Tecnología Blockchain

El sistema blockchain podría ayudar a disminuir el alto nivel de exclusión financiera y económica y de informalidad empresarial y laboral que existe en los países en desarrollo, producto de los costos burocráticos, la ineficiencia del Estado e instituciones débiles. Esta tecnología podría ser la solución ya que facilita la creación de nuevos modelos de empresa y la inclusión financiera, dando acceso al ahorro y haciendo factible la entrega de microcréditos a personas excluidas del sistema financiero tradicional.

La tecnología blockchain dota a las personas y a las pequeñas empresas de todo el mundo de muchas de las funciones y capacidades que tienen las empresas más grandes. Primero, hace rentable micro operaciones que en el sistema tradicional no serían factibles debido a su alto costo productor de los intermediarios involucrados y la infraestructura utilizada. Además, los archivos y registros blockchain y los contratos inteligentes facilitan la creación de una empresa, aceleran los trámites legales y ahorran papeleo, sobre todo en los países en vías de desarrollo, donde los costos y el tiempo necesario para constituir una empresa son más altos que en los países desarrollados. Así también, esta tecnología puede ayudar a garantizar los derechos de autor y facilitar la gestión de derechos digitales de propiedad.

3.1 Contratos inteligentes

El uso de la tecnología blockchain y de los contratos inteligentes que esta tecnología permite utilizar tiene el potencial de generar desarrollos, aplicaciones y soluciones en diversas áreas e industrias como transporte, gestión de infraestructuras, gestión de energía, residuos y servicios básicos, extracción de recursos, agricultura y ganadería, control medioambiental y servicios de emergencia, atención sanitaria, servicios financieros y seguros, archivo de documentos y registros, administración de propiedades, operaciones industriales, administración del hogar, y operaciones y ventas al por menor, entre otros¹⁶.

Hoy en día, en las áreas e industrias mencionadas, se utilizan dispositivos inteligentes que prestan servicios, pero pocos de éstos pueden comunicarse entre sí (solicitarse información o recursos y pagarse por ellos), teniendo en cuenta lo importante que es proteger la privacidad de las personas involucradas, ya sea como consumidores, pacientes, trabajadores, etc.

Además, gracias al desarrollo de contratos inteligentes, es posible automatizar muchos aspectos del funcionamiento de una empresa. Así, surgen dos nuevos modelos de negocio para la empresa individual:

- Compra y venta de capacidad ociosa o sobrante.
- Micro rentabilización de información.

¹⁶ Para más detalles, ver Tapscott y Tapscott (2017).

3.1.1 Gestión de la ayuda humanitaria

Como se mencionó anteriormente, los criptopagos permiten la disminución de los costos de envío de remesas y así, su factibilidad en el caso de montos pequeños. Así también, la tecnología blockchain puede mejorar la gestión de la ayuda extranjera de dos maneras. Primero, al prescindir de intermediarios que manejen la transferencia de grandes sumas de dinero, puede reducir el problema crónico de malversación y robo. Segundo, siendo un registro inmutable del flujo de capitales, obliga a las instituciones, de organizaciones humanitarias a gobiernos, a actuar con integridad y cumplir con sus compromisos. Si no lo hacen, la gente podrá ver sus malas acciones y pedirles cuentas de ellas.

La ayuda por catástrofes naturales o contra la pobreza no puede brindarse siempre de persona a persona, claro está. Además, en muchos casos, las instituciones no sólo son deseables sino también fundamentales. Pero esta tecnología podría aumentar radicalmente el nivel de transparencia con la que esas organizaciones, y otras instituciones de la cadena de valor de la ayuda extranjera, funcionan. De hecho, estos contratos inteligentes permiten hacer seguimiento de recursos o ir liberándolos paulatinamente según se cumplan condiciones de identidad, avance de proyectos o asistencia, por ejemplo. Así también permite realizar un registro de propiedades más confiable y seguro, lo que puede facilitar la focalización en la entrega de ayuda.

3.2 Estonia, país digital

Evidentemente, la tecnología blockchain no sólo sirve para empresas que buscan beneficios, sino también para instituciones públicas que trabajan por la prosperidad de todos, tanto en el ámbito del gobierno, la educación y la sanidad como en el de las redes energéticas, los sistemas de transporte y los servicios sociales.

Estonia, por ejemplo, ha diseñado su estrategia de gobierno digital basándose en la descentralización, la interconectividad, la apertura y la seguridad cibernética. El objetivo es crear una infraestructura duradera que se adapte a lo nuevo. Todos los residentes tienen acceso a la información y a los servicios en línea, pueden usar sus identidades digitales para hacer negocios y actualizar o corregir sus datos en los registros estatales y de propiedad. Aunque gran parte de esta labor es anterior al sistema blockchain, el país introdujo una infraestructura de firma sin clave que se integra perfectamente con la tecnología blockchain.

Así también, construyeron esta tecnología para que todo lo que hubiera en las redes estatales pudiera verificarse, por lo que al gobierno le es imposible mentir a sus ciudadanos. Este sistema garantiza niveles de transparencia y responsabilidad totales; todos pueden ver quién introduce qué información, cuándo la introduce y qué hace con ella. En consecuencia, el Estado puede demostrar la integridad de sus registros y el cumplimiento de las leyes, y los ciudadanos pueden verificar la integridad de sus propios registros sin necesidad de que intervenga un tercero. Esto reduce los costos, ya que no hay claves que proteger ni documentos que volver a firmar periódicamente. Así también, garantiza la privacidad y el derecho a propiedad. Todo esto hace que Estonia gane competitividad en la economía global, atrayendo negocios e inversiones.

Por lo demás, tiene el potencial de mejorar la democracia, a través de hacer más confiable y transparentes los sistemas de votos, conteo y votaciones electrónicas, lo que además evita ejercer presión sobre minorías.

3.3 Ofertas Iniciales de Monedas (ICOs)

En plena era digital, las ICOs (Ofertas Iniciales de Monedas) surgieron como una nueva forma de recaudar fondos de capital gracias a las monedas digitales y a la tecnología blockchain, en la que los participantes invierten dinero *fiat*¹⁷ y reciben a cambio "*tokens*" o activos digitales. Una persona, proyecto o empresa que necesita capital crea un nuevo tipo de moneda digital y vende una porción de la misma por monedas *fiat* en una plataforma comercial o de intercambio digital.

En palabras simples, las ICOs son ofertas a medio camino entre el *crowdfunding* y una salida a Bolsa, pero siempre usando la tecnología blockchain o cadena de bloques, la cual está detrás de las criptomonedas como el Bitcoin. Así, los que invierten en una ICO no se convierten en accionistas tradicionales, sino que a cambio de su dinero reciben *tokens* o una moneda digital creada para tal efecto. Estos *tokens* pueden servir para adquirir los bienes o servicios que la compañía en cuestión va a ofrecer, pero también se pueden usar como una moneda fácilmente intercambiable. En otras palabras, estos *tokens* son intercambiables por servicios o activos, o se pueden retener con fines especulativos. Se explica en detalle a continuación.

Una ICO consiste en un evento, regularmente denominado "*crowdsale*", en que una empresa libera su propia criptomoneda con el propósito de obtener financiamiento. Por lo general, libera un cierto número de *cripto-tokens* y luego vende esas "fichas virtuales" a su público objetivo, más comúnmente a cambio de Bitcoins, pero también puede ser a cambio de dinero fiduciario o *fiat*.

¹⁷ Dinero *fiat* es la forma de dinero fiduciario cuya principal característica es que no tiene valor intrínseco. Su valor proviene del respaldo legal y el acuerdo social en torno al valor de la moneda.

Como resultado, la compañía obtiene el capital necesario para financiar el desarrollo del producto y los inversionistas obtienen acceso a lo que les permitan hacer sus *cripto-tokens*. Además, tienen la propiedad completa de estas “acciones”.

El *crowdsale* generalmente ocurre antes de que un proyecto haya lanzado oficialmente su servicio, y está diseñado para generar fondos para el desarrollo del proyecto, lo que ayuda a pagar a los desarrolladores de software, los presupuestos de marketing y todas las demás cosas que necesita una *start-up*. También se puede usar para medir el interés en un proyecto en particular. Si nadie compra los *tokens*, entonces la compañía que está desarrollando el proyecto podría querer reconsiderar sus opciones.

3.3.1 Diferencias entre ICO e IPO¹⁸

Si bien existen algunas similitudes entre los conceptos de Oferta Pública Inicial e ICO, también hay importantes diferencias entre ambos. Por un lado, las acciones de una empresa, publicadas durante una IPO, siempre representan cierta participación en la propiedad de la empresa respectiva. Esto no siempre ocurre en el caso de las *cripto-fichas* que se venden al público en un ICO. Las *cripto-fichas* se pueden utilizar para transferir poderes de voto (una proporción mayor de fichas da más poder de voto) en algunos proyectos, pero más a menudo estas fichas son sólo eso: unidades de dinero que pueden enviarse a otros usuarios e intercambiarlas por otras monedas.

Otra importante diferencia es que las IPOs están fuertemente reguladas por las autoridades. Esto implica que una empresa partícipe debe preparar una gran cantidad de documentos antes de liberar sus acciones¹⁹. También conlleva severas consecuencias en caso de incumplimiento. Por otra parte, el *crowdfunding* de la criptomoneda está recién siendo un tema en el ámbito de la regulación. Esto significa que cualquier proyecto puede lanzar una ICO en cualquier momento con poca preparación y cualquier persona puede participar en él y contribuir con su dinero, sin importar de qué país sea.

Claramente, esto trae nuevas oportunidades, pero también nuevos riesgos en comparación con las IPOs más conservadoras. Debido a que actualmente se trata de un mercado poco o ligeramente regulado, existen pocos requisitos legales para la empresa y pocas protecciones legales para el comprador. Esto puede tener ventajas en el costo y en la complejidad de la recaudación de fondos para la empresa y además posibilita que inversores minoristas apoyen a las compañías.

¹⁸ IPO es un término bursátil que significa Oferta pública inicial y se utiliza para hacer referencia al lanzamiento de las acciones de una empresa en el mercado de valores cuando están disponibles para el público.

¹⁹ Por ejemplo, en Estados Unidos, para realizar una oferta pública de acciones, la compañía debe de incorporarse como sociedad anónima (de acciones), además de registrarse con la comisión de valores, SEC (Securities and Exchange Commission). Además, debe publicar una cantidad de información extensa, incluyendo los reportes financieros. Todo esto dificulta el proceso de atraer inversiones en el proyecto en una etapa inicial, no obstante, otorga ciertas garantías a los inversores.

Finalmente, en algunos casos, las garantías legales, como por ejemplo la propiedad legal de un determinado porcentaje de una compañía atribuida a las personas que poseen sus acciones, se sustituyen por garantías criptográficas, como por ejemplo contratos inteligentes que distribuyen automáticamente una parte de los ingresos a los poseedores de *tokens* cada vez que se hace un pago y antes de que el dinero llegue incluso a las manos de su compañía.

3.3.2 Beneficios potenciales de las ICOs

El objetivo principal de una ICO es el financiamiento de un proyecto en particular. Sin embargo, hay oportunidades adicionales de obtener beneficios en el proceso.

En la mayoría de los casos, las cripto-fichas liberadas durante una ICO se venden a un precio fijo en Bitcoins o en dólares estadounidenses. Ese precio no está respaldado por nada más que la confianza en que el equipo de desarrollo logre lanzar un producto terminado en algún momento en el futuro, por lo que suele ser bastante bajo. Después de que el proyecto se desarrolla y se pone en marcha, el valor de las fichas se garantiza con un producto real y funcional. Y eso casi siempre conduce a un aumento en el precio.

Cuando esto sucede, los patrocinadores originales pueden vender sus fichas con un beneficio sustancial.

Por ejemplo, durante la ICO de Ethereum en 2014, las fichas se vendieron a un precio que oscilaba entre 0,3 y 0,4 dólares por ficha. Después de que la plataforma principal del proyecto fue lanzada en julio de 2015, el precio de cada ficha había aumentado significativamente, alcanzando los US\$19,4. Esto significa que algunos de los participantes pudieron reclamar un ROI de más de 6.000%.

Sin embargo, los beneficios no están garantizados. Una campaña de ICO puede fallar. Incluso si tiene éxito, existe la posibilidad de que los desarrolladores no sean capaces de entregar un producto final y el precio de las fichas nunca subirá. Este es un riesgo que todos los participantes de una ICO tienen que tener en cuenta cuando deciden contribuir a cualquier campaña.

3.3.3 Regulación de ICOs en el mundo

La reglamentación mundial de las ICOs ha sido desigual, con China y Corea del Sur en un extremo del espectro reglamentario prohibiendo todas las ICOs en el país en 2017, mientras que otros países como Suiza, Singapur y Australia han proporcionado directrices con el fin de apoyar a las ICOs conforme con la legislación vigente en cada país.

A medio camino se encuentran Reino Unido y Estados Unidos, que son territorios con un alto despliegue de ICOs y de todo tipo de actividades relacionadas con la cadena de bloques, pero con una gran falta de claridad jurídica.

Reino Unido, al igual que Singapur, cuenta con un componente regulador para evaluar los nuevos proyectos financieros, y la Autoridad de Conducta Financiera de Reino Unido (FCA) tiene la postura de esperar cómo avanza la tecnología de contabilidad distribuida. En este país las criptomonedas se consideran “monedas privadas”, y en lo referente a las ICOs, los emisores están actuando de acuerdo con su propia interpretación de los parámetros legales.

En el caso de Estados Unidos abundan los reguladores, lo que hace que la emisión de *tokens* se torne compleja. No obstante, alrededor de 50 estados individuales han implementado sus propias reglas, como New York y Delaware: el primero con su ley llamada “BitLicense”, y el segundo, considerado el nuevo hogar estadounidense para la economía basada en las criptomonedas, recientemente introdujo una variedad de leyes relacionadas con la tecnología blockchain. En todo caso, las directrices relacionadas con el tema aún se consideran insuficientes y todas pertenecen sólo al ámbito bancario.

La mayoría de los reglamentos de las ICOs a nivel mundial incluyen una advertencia a los inversores sobre la posibilidad de que se produzcan fraudes al participar en esta nueva forma de recaudación de fondos. De todas formas, en el caso de Suiza por ejemplo, se advierte sobre los riesgos asociados con las ICOs en términos de la volatilidad de precios del mercado y la naturaleza legal potencialmente incierta de los contratos celebrados con la tecnología blockchain.

3.3.3.1 Regulación en Suiza

En febrero de este año, la Autoridad de Supervisión del Mercado Financiero Suizo (FINMA)²⁰ implementó un marco que regula las criptomonedas, el uso de la tecnología blockchain y las tecnologías de libro mayor distribuidas. Así, Suiza se posiciona como uno de los ecosistemas líderes a nivel global para el uso de estas tecnologías.

Mientras que los reguladores de otros países – entre ellos Chile - no dejan de postergar la aplicación de medidas en torno a las criptomonedas, durante 2017 Suiza, a través de la FINMA, creó una guía en que se reconoce el potencial innovador de esta tecnología, y reitera que, en los últimos años, la máxima autoridad financiera del país ha apoyado los esfuerzos en el desarrollo de soluciones basadas en la cadena de bloques²¹.

²⁰ La FINMA se encarga de supervisar los bancos, bolsas de valores, compañías de seguros y todos los agentes financieros en Suiza.

²¹ Cabe destacar que, en 2002, Suiza aprobó una normativa que se denominó “neutralidad tecnológica”, que hacía legales a nivel jurídico los medios electrónicos cuando son usados para fines administrativos. Es por este motivo, que algunos aspectos de las ICOs pueden ser vinculados a la legislación de Suiza, con respecto a la función de los servicios prestados por los ofertantes.

Durante 2017, las ICOs con sede en Suiza recaudaron cerca de \$550 millones de dólares en financiamiento, lo que representó el 14% del mercado mundial de las ICOs. El inconveniente es que muchas de las ICOs suizas se estructuraron como fundaciones que quedaron calificadas con un estatus fiscal sin fines de lucro y en el que el dinero recaudado en estas ICOs era tratado como una donación que no puede ser devuelta a los inversionistas.

En respuesta al fuerte aumento del número de ICOs suizas y a la falta de claridad y transparencia sobre cómo o si deben ser reguladas²², y con la intención de proteger a los inversionistas²³ y la integridad del sistema financiero, en febrero de este año, la FINMA publicó directrices para las ICOs.

FINMA declaró comprender que no todas las reglas que se aplican a los mercados financieros son aplicables a la oferta inicial de monedas. El informe indica que cada *crowdsale* tiene su propia singularidad según cómo se haya estructurado. En consecuencia, las directrices explican que las ICOs se evaluarán caso por caso, dependiendo de su diseño.

La Agencia, en un intento por clasificar los *tokens*, declaró que se haría hincapié en su utilidad y transferibilidad teniendo en cuenta las leyes anti lavado de dinero del país. Con el fin de evaluar futuras ICOs y determinar qué leyes aplican, FINMA divide los *tokens* de ICO en tres categorías: *tokens* de pago, *tokens* de servicios públicos y *tokens* de activos. Esto significa que no se ha establecido una regulación específica de ICO en Suiza, sino que la autoridad reguladora ha concluido que para evaluar a los *tokens* reconocerán tres categorías que dependen de la función y transferibilidad de los mismos.

El primer tipo de *token* que FINMA reconoce son aquellos que están diseñados como métodos de pago y no están enlazados a ningún proyecto. Según lo establecido, un *token* será considerado “de pago” cuando sea “sinónimo de criptomonedas y no tenga funciones adicionales”; además debe ser transferible. Para las Ofertas Iniciales de Moneda que estén relacionadas con el uso de este tipo de *token*, la autoridad del mercado financiero exigirá que se cumplan con las normas contra lavado de dinero²⁴, esto a pesar de que no reconocerá a los criptoactivos originados del proceso ICO como un valor.

²² El organismo suizo sostiene que “La aplicación de la tecnología blockchain tiene un potencial innovador dentro y más allá de los mercados financieros. Sin embargo, los proyectos basados en esta tecnología realizados de manera análoga a las actividades reguladas no pueden eludir simplemente el marco regulatorio probado”.

²³ La naturaleza no regulada de las ICOs ha sido motivo de preocupación para los inversionistas y los reguladores. De hecho, se informó que en 2017 el 10% de todos los fondos de ICO se perdieron debido a fraudes y empresas fraudulentas.

²⁴ La ley contra el blanqueo establece, entre otros requisitos, la necesidad de identificar a los beneficiarios para proteger al sistema de delitos de “lavado” y financiación del terrorismo.

Los *tokens* de utilidad son los segundos en el esquema regulatorio que las autoridades en Suiza pretenden establecer. Estos están “destinados a proporcionar acceso a una aplicación o servicio”, razón por la cual no califican como activos. Sin embargo, de tratarse de un caso en el que los *tokens* de utilidad ofertados funcionen como inversión -bien sea de forma parcial o total- sí serán considerados como un valor.

Por último, se encuentran los *tokens* de activos: estos representan activos con respaldo físico real, activos en compañías que prometen retornos como pagos de intereses, flujos de ganancias o derechos a dividendos. En estricto rigor, estos adquieren la condición de activo, pero su compra y venta están sujetos a las obligaciones del Código Civil suizo y la Ley de Valores²⁵. En resumen, este tipo de *tokens* representan un activo tal como una acción, un bono o derivados, por lo que se considerarán valores (*securities*, en inglés).

En resumen, a partir de las directrices regulatorias publicadas, muchas ICOs serán consideradas valores. Sin embargo, se establecieron algunas excepciones. Por ejemplo, los *tokens* utilizados para acceder a una plataforma que ya está en funcionamiento, o para criptomonedas que funcionan sólo como medio de pago, no se considerarán valores, al igual que los *tokens* sujetos a la regulación anti lavado de dinero.

Con respecto a las licencias de operación, la FINMA podrá solicitar una licencia bancaria especial cuando los ofertantes de ICO acepten depósitos bancarios. En el caso del mercado de valores, si los *tokens* pueden ser identificados como valores (por ejemplo, derivados), entonces se necesitará una licencia especial para comerciar con ellos. Asimismo, si los activos recolectados en una ICO son gestionados externamente, entonces aplicarán las leyes para los planes de inversión colectiva.

Este nuevo marco regulatorio establece que las criptomonedas no son dinero ni una moneda, ni una oferta financiera para fines de impuesto sobre bienes y servicios (GST). Así, las transacciones con *tokens* que califiquen como valores pueden quedar afectas al impuesto sobre las transferencias de valores para instrumentos nacionales a una tasa del 0,15% (o del 0,30% para instrumentos no nacionales) en los casos en que un corredor de valores suizo haya participado en la transacción.

De esta forma, las criptomonedas pasan a ser un activo para fines del impuesto sobre las ganancias de capital (CGT), que sólo se aplica a quienes califican como *traders* profesionales. Los tenedores o inversionistas de criptomonedas están sujetos a un impuesto al patrimonio a la tasa determinada por las autoridades fiscales a fines del año fiscal.

²⁵ Esta ley busca garantizar que los participantes en el mercado puedan tomar sus decisiones de inversión en base a un conjunto mínimo de información fiable con el fin de que el comercio sea justo para las partes.

Por ejemplo, un *token* de patrimonio, emitido por una ICO, puede estar sujeto a un impuesto de capital único del 1%, a diferencia de un *token* de deuda. Cualquier distribución de beneficios sobre *tokens* de patrimonio o pagos sobre *tokens* de deuda está sujeta a la retención de impuestos suiza a una tasa del 35%.

3.3.4 Futuro de las ICOs

Aún no está claro si la tecnología blockchain eliminará los intermediarios financieros y sus comisiones, o si simplemente introducirá una nueva clase de intermediarios. Sumado a esto, las burbujas especulativas e irracionales en las criptomonedas podrían generar inestabilidad en el sistema financiero en su conjunto. Por esto, es comprensible que algunos reguladores opten por prohibirlas.

Sin embargo, el mercado de capitales en general, y el financiamiento y la recaudación de capital en particular, son mercados que requieren ser competitivos para su buen funcionamiento. A partir de esta premisa, no se debería rechazar de antemano ninguna nueva tecnología o innovación que tenga el potencial de introducir más competencia al mercado, o bien, que sea capaz de disminuir los costos de operación. Por lo tanto, en principio, hay mucho para decir a favor del enfoque de Suiza.

El desafío radica en que la generación de *tokens* (o criptomonedas) estandarizados es uno de los procesos más simples que se pueden desarrollar en plataformas como Ethereum y que hay mucha gente dispuesta a comprar sin entender ni discriminar lo que se le ofrece, como también hay otros que vieron aquí la oportunidad de abusar. Como las representaciones de valor son idénticas, por diferente que sea lo representado, se confunden ventas de participación en empresas, ventas de eventuales servicios futuros, venta de unidades de valor en sistemas de pago y venta de humo, todo bajo el rótulo de ICO. Es por lo anterior que la regulación de estas tecnologías toma tal preponderancia en los mercados financieros actuales, teniendo presente el desafío de no frenar la innovación tecnológica que tantos beneficios puede entregar al desarrollo económico.

4. Blockchain dentro del Marco de la Irrupción de FinTech: Desafíos para la Banca Central

De acuerdo con Levine (2017), las instituciones, los servicios y el desarrollo financiero en general, juegan un rol fundamental en el crecimiento y desarrollo económico, ya que permiten movilizar ahorros y reunir fondos para hacer posibles grandes proyectos de inversión, asignar capital de forma eficiente y proporcionar mecanismos y servicios para gestionar y administrar el riesgo.

A partir de lo anterior, la irrupción de las innovaciones financieras facilitadas por la tecnología, en adelante denominadas FinTech²⁶, adquiere importancia ya que éstas tienen el potencial de cambiar la prestación de servicios financieros en el futuro próximo.

El paper que se sintetiza a continuación -Furche et al. (2017)- fue escrito por cuatro economistas del Banco Central de Chile y aborda la reciente irrupción de las FinTech. En particular, se analiza cómo estas innovaciones pueden afectar la provisión de servicios financieros en economías en desarrollo y el rol de los bancos centrales como agentes reguladores y responsables de la estabilidad financiera.

Dado que una fracción importante de la población en países de bajos ingresos aún carece de acceso a servicios formales de instituciones financieras, las innovaciones FinTech tienen el potencial de proveer estos servicios y así tener un impacto positivo en la inclusión financiera de dichos países²⁷. Sin embargo, estas innovaciones financieras también pueden alterar la transmisión de la política monetaria, cambiando el rol de los agregados monetarios y el sistema bancario, lo que implica ciertos riesgos para la estabilidad financiera.

²⁶ El Consejo de Estabilidad Financiera (2017) concibe “FinTech” como las innovaciones en servicios financieros facilitadas por la tecnología que podrían traducirse en nuevos modelos de negocios, aplicaciones, procesos o productos, con un efecto material asociado en la prestación de servicios financieros. Las innovaciones FinTech se refieren a un amplio campo de productos y servicios, considerando desde las criptomonedas a los mecanismos de financiamiento colectivo (*crowdfunding*), pasando por préstamos persona a persona (P2P lending) y la inteligencia artificial.

²⁷ Las FinTech pueden contribuir al desarrollo financiero de los países emergentes facilitando o permitiendo:

- i) el acceso universal a los servicios financieros por parte de los consumidores y las pequeñas y medianas empresas;
- ii) mayor seguridad en las remesas y transacciones entre personas con menores ingresos, migrantes y habitantes de las áreas rurales;
- iii) mayor competencia y menor concentración del sector financiero, y
- iv) reducción en los costos, producto de la participación en la economía formal y mejor acceso a los servicios públicos gracias a bases de datos estatales mejoradas.

En algunos casos, las FinTech pueden además competir con proveedores financieros tradicionales en áreas como los sistemas de pago, el comercio, la custodia, la administración de activos y la intermediación de préstamos. Por esta razón, la regulación y la formulación de políticas públicas deben adaptarse a los desafíos planteados por las nuevas tecnologías y, a la vez, asegurar que éstas no se transformen en barreras a posibles innovaciones.

4.1 Rol de los bancos centrales

Los bancos centrales cumplen funciones de enorme relevancia en el ámbito de la regulación, la supervisión, el manejo de liquidez y como prestamistas de última instancia. Si bien la mayoría de los bancos centrales tiene como principal mandato la estabilidad de precios y tienen metas explícitas de inflación, tienen también responsabilidad respecto de la estabilidad financiera y su supervisión. Dentro de las responsabilidades relacionadas con la estabilidad financiera, se pueden incluir la regulación y supervisión bancaria²⁸, el establecimiento de normas sobre seguros de depósitos, la provisión de redes de seguridad a través de asistencia de fondos de liquidez de emergencia, la prestación de servicios de corretaje y el involucramiento en el sistema de pagos en general (Banco de Pagos Internacionales 2009).

Así, para cumplir con los mandatos de estabilidad monetaria y financiera, los bancos centrales aplican, a la vez, una política monetaria, y regulaciones macrofinancieras en materia de liquidez, reservas y/o requerimientos de capital, por ejemplo. A su vez, la transmisión de la política monetaria puede amplificarse por su impacto sobre el crédito a través de dos canales que afectan la prima de financiamiento exterior: el canal de los balances y el de los préstamos bancarios²⁹.

²⁸ En muchos países, tanto los bancos como los intermediarios financieros no bancarios son regulados y supervisados por otras autoridades que son autónomas del banco central (Raddatz y Vergara 2016). Considerando el rol creciente de las regulaciones macroprudenciales de los bancos y de los intermediarios financieros no bancarios en la transmisión de la política monetaria (Fondo Monetario Internacional 2016) y el acceso al crédito por parte de las empresas y los consumidores (Raddatz y Vergara 2016), es probable que el crecimiento de las FinTech potencie la relevancia de la coordinación del banco central con otros reguladores financieros.

²⁹ El canal de hoja de balance —es decir, el efecto financiero de la política monetaria en las cuentas de balance de las empresas— pone el acento en el impacto de la política monetaria en el valor neto de los deudores, su solvencia crediticia y garantías, mientras que el canal de los préstamos bancarios se centra específicamente en la transformación de los depósitos y las reservas en préstamos. De acuerdo con Bernanke y Gertler (1995), el canal de préstamos bancarios —cuya base está en que la política monetaria opera fundamentalmente mediante el volumen de crédito bancario— es usualmente menos relevante para la mayoría de los ciclos de negocios, pero su rol toma importancia durante las crisis financieras en las que los bancos enfrentan la escasez de fondos.

Aquí, es importante señalar que la transmisión de la política monetaria puede verse afectada por las percepciones de riesgo e incertidumbre o por situaciones que afecten la confianza en una economía. Por esta razón, aun cuando los productos financieros basados en nuevas tecnologías tienen el potencial de mejorar la calidad y velocidad de los servicios financieros, o reducir su costo, un banco central tenderá a enfocarse en los riesgos que implica el uso de estas nuevas tecnologías y su eventual impacto en el sistema financiero.

4.2 Oportunidades que entrega FinTech: Contribuciones, riesgos potenciales y desafíos

Hoy en día, la mayor disponibilidad de datos y los avances en materia de programación, encriptación y dispositivos móviles tienen el potencial de desagregar funciones que eran típicamente bancarias, como los pagos y la asignación de capital.

Para poder comprender el impacto potencial de las FinTech sobre la banca central, primero identifiquemos los principales desarrollos de las innovaciones FinTech. Así, podremos analizar los efectos sobre la política monetaria y la estabilidad financiera en cada tipo de innovación. Éstas se presentan en la Tabla N°1.

A partir de esta tabla, es posible mencionar que las innovaciones FinTech pueden traer consigo importantes beneficios para la estabilidad financiera. Por ejemplo, el financiamiento colectivo y la intermediación entre pares (P2P)³⁰ pueden reducir el riesgo sistémico, en la medida que no impliquen la creación de dinero a través del mecanismo convencional de transformación de madurez y multiplicador monetario de los bancos.

Por otro lado, las herramientas FinTech también pueden contribuir a la estabilidad financiera, en la medida en que puedan generar más información para evaluar el riesgo crediticio y mitigarlo a través de contratos, garantías y avales eficientes. La inteligencia artificial (IA), por ejemplo, puede acelerar los asuntos legales y de auditoría más rutinarios, permitiendo que los agentes puedan lidiar con los riesgos más inesperados (Brennan et al. 2017). Así también, Deloitte (2016) afirma que la IA puede tener un impacto similar sobre la industria legal, al permitir preaprobaciones automatizadas de contratos y una predicción más exacta de los riesgos derivados de las decisiones de los tribunales y de los conflictos legales con terceros.

Así también, la inteligencia artificial puede mejorar la experiencia del cliente en el comercio minorista y facilitar la comprensión por parte de los auditores o reguladores de los contratos establecidos por las empresas. Además, la IA puede ayudar a los pequeños inversionistas a detectar errores frecuentes que cometen en términos de una excesiva carga de deuda o una falta de diversificación en su portafolio.

³⁰ Un servicio entre pares (P2P) es una plataforma descentralizada en la que dos individuos pueden interactuar de manera directa sin la intermediación de terceros. Así, un comprador y un vendedor pueden transar directamente a través de los servicios P2P. Algunos servicios P2P no implican una transacción económica, como comprar y vender, sino que reúnen individuos en torno a proyectos comunes, información compartida o para comunicarse sin intermediarios.

Tabla N°1: Desarrollos FinTech, su innovación y su potencial contribución

Actividad	Innovación en el producto	Contribución potencial
Pagos, transferencias y liquidaciones	Pagos móviles, billeteras digitales, divisas digitales y contabilidades distribuidas	Manejo de numerosas transacciones con costos operacionales más bajos. Menores requerimientos de garantías
Obtención y concesión de préstamos; intermediación financiera	Financiamiento colectivo, plataformas digitales de préstamos P2P. Mayor uso de grandes bases de datos para calificación de crédito.	Las FinTech aún representan una pequeña porción del crédito total, pero está creciendo rápidamente en algunos países. Una mejor evaluación de riesgo puede abrir acceso a segmentos de mercado no cubiertos en la actualidad.
Manejo de riesgos	Compañías de seguro FinTech: InsurTech. Contabilidades distribuidas: registro de garantías y avales en transacciones.	Mejoras en el marketing, la distribución, suscripción, valoración del riesgo y resolución de reclamaciones.
Apoyo al mercado	Verificación de identidad, computación en "la nube", activos digitales y notarios en línea.	Registros más expeditos y exactos. Menores costos burocráticos y de custodia. Encriptación de datos sensibles.
Manejo de inversiones	Plataformas de comercio electrónico, asistentes robóticos, contratos inteligentes.	La asesoría automatizada puede complementar a los asistentes humanos, aumentando el valor de las inversiones.
Auditoría y aspectos legales	Revisiones mediante inteligencia artificial, consejería legal automatizada.	Las auditorías con inteligencia artificial permiten revisar grandes volúmenes de documentos para detectar eventuales errores. Los algoritmos pueden preaprobar los contratos y predecir decisiones legales basadas en documentos anteriores.
Apoyo al cliente	Inteligencia artificial, asistentes inteligentes.	Los asistentes inteligentes pueden ayudar a los clientes a comprender errores pasados y riesgos futuros de sus finanzas.

Fuente: Furche et al. (2017)

Adicionalmente, es posible afirmar que las aplicaciones de la IA presentan un bajo riesgo para la estabilidad financiera, puesto que sus algoritmos buscan imitar las mejores estrategias humanas posibles o corregir errores humanos basados en datos pasados. Por ende, es poco probable que la IA genere peligros o riesgos que no estén ya presentes en el comportamiento humano.

Sin embargo, otros desarrollos de las FinTech sí pueden implicar riesgos para la estabilidad financiera y la transmisión de la política monetaria. Quizás el mayor de estos riesgos dice relación con el nivel de ciberseguridad³¹. Mientras más dependan los sistemas financieros de plataformas electrónicas y de registros digitales, más expuestos estarán a ciberataques que pueden alterar los flujos de fondos, información, aprobaciones, entre otros.

Por el lado de los desafíos, tenemos que el uso masivo de los desarrollos FinTech requiere mayores inversiones en educación y alfabetización financiera. La experiencia reciente muestra que incluso en los países desarrollados las personas suelen hacer un mal uso de los instrumentos financieros. En esta línea, Haliassos (2015) sostiene que los consumidores, por lo general, padecen de grandes cargas de deuda y contratos complejos que no comprenden a cabalidad; o compran productos inadecuados, con excesivo riesgo, baja diversificación y/o altos costos. Adicionalmente, el uso de estos nuevos servicios digitales podría requerir una mejor infraestructura de internet y telecomunicaciones.

En el sistema tradicional, el Estado tiene el monopolio de la producción de dinero. ¿Qué pasaría si el dinero no lo emitiera exclusivamente una autoridad central, sino que éste fuera (al menos en parte) creado por una red distribuida mundial? Esto implicaría importantes desafíos para la banca central en sus tres misiones fundamentales que son la estabilidad monetaria, la estabilidad financiera y la regulación de instituciones financieras.

En la misma línea de riesgos y desafíos, surgen las criptomonedas generadas por privados, que son un desarrollo que podría reducir el uso de las divisas oficiales y dificultar el monitoreo de los agregados monetarios, lo que se traduce en un desafío para la política monetaria. Además, la volatilidad de precios de las monedas virtuales y el riesgo de corridas causadas por la pérdida de confianza podrían llegar a debilitar el rol de la banca central como proveedora de liquidez y prestamista de última instancia. Además, las divisas digitales pueden también facilitar la evasión de impuestos, los fraudes y las transacciones ilegales, por lo que es preciso fortalecer las leyes en este ámbito.

Otro importante desafío que se presenta con la irrupción de las FinTech es que cabe la posibilidad de que generen una reducción en el número de trabajadores necesarios para la industria financiera. Algunos trabajos podrían volverse obsoletos con la tecnología. Además, los efectos de equilibrio general de estos cambios son difíciles de predecir. Sin embargo, como bien postula Furche et al. (2017), la evaluación de riesgos financieros siempre implica poner atención en factores nuevos e impredecibles, algo que las personas tienden a hacer mejor que las máquinas. Asimismo, las características específicas de las regulaciones financieras e inversiones en las industrias de los diferentes países hacen que sea poco probable, en el mediano plazo, un remplazo total de la intermediación financiera por nuevos desarrollos tecnológicos.

³¹ Naturalmente, este riesgo no es exclusivo de los desarrollos FinTech, sino que de cualquier sistema financiero electrónico.

4.3 Impacto potencial de las tecnologías de contabilidad distribuida y de cadena de bloques (blockchain)

Probablemente, la cadena de bloques y, en términos más amplios, la tecnología de contabilidad distribuida es el desarrollo más revolucionario en FinTech y el con mayor potencial para redefinir el sistema financiero y la banca central.

Esta tecnología tiene el potencial de mejorar la eficiencia de las infraestructuras del mercado financiero al incrementar la velocidad de la resolución de las transacciones, lo que reduce las necesidades de garantías y aumenta la liquidez, a la vez que aminora los costos operacionales y de servicios. Lo analizaremos en detalle a continuación.

Por lo general, la creación de un activo financiero requiere una contraparte central de confianza (por ejemplo, un banco central) que actuará como intermediario para todas las transacciones. Las tecnologías de contabilidad distribuida y de cadena de bloques conservan un registro de todas las transacciones y los títulos de propiedad de los activos de la red, que es monitoreado por todos los agentes; por lo tanto, no es posible engañar a sus miembros realizando una operación en que el mismo activo, moneda o garantía, es comprometido con diferentes partes. Esto implica que la tecnología de contabilidad distribuida puede ser utilizada para crear cualquier tipo de contrato financiero, activo o moneda digital, porque sus activos digitales gozarán de la confianza de todos los miembros de la red.

La tecnología de contabilidad distribuida puede potenciar la eficiencia de los sistemas de pago, ya que todos los procesos de liquidación y pago de órdenes son implementados en tiempo real, mientras que en la actualidad la mayoría de los procesos de liquidación requieren dos a tres días, lo que crea riesgos operacionales y relacionados con la contraparte.

Con respecto a la estabilidad financiera, entre los potenciales beneficios de la tecnología de contabilidad distribuida, se pueden destacar:

- i) una mayor eficiencia de mercado, en particular para los sistemas de liquidación bruta en tiempo real dentro de las grandes instituciones financieras;
- ii) una mejor medida del riesgo para cada banco y un sistema financiero más transparente;
- iii) menores costos comerciales, robustez frente a los ciberataques y menor necesidad de garantías.

En el caso del intercambio de valores, las tecnologías de contabilidad distribuida podrían reemplazar un sistema complejo con muchas capas institucionales y con diferentes bases de datos. En estos casos, la tecnología de contabilidad distribuida crearía una sola transacción y actualizaría una sola base de datos que sería inmediatamente reconocida por todos los integrantes de la red, lo que reduce los costos de transacción y las demoras en comunicación entre todos los agentes.

Finalmente, un mercado basado en la tecnología de contabilidad distribuida puede también ayudar a mejorar la transmisión de la política monetaria, debido a su alta transparencia (facilitando el canal de la toma de riesgo), y a reducir las necesidades de garantías (lo que fortalece el canal de balances). Más aún, de acuerdo con Philippon (2017), la arquitectura financiera simplificada podría aminorar el rol de los actores actuales y la importancia de las instituciones “demasiado grandes para quebrar”.

4.4 Bancos centrales y la posibilidad de crear sus propias monedas digitales³²

Es posible que la creación de monedas digitales por parte de los bancos centrales sea el proyecto más ambicioso para un sistema basado en tecnologías de contabilidad distribuida. De acuerdo con Raskin y Yermack (2016), el uso de monedas digitales de los bancos centrales podría traer algunas ventajas para sus usuarios como:

- i) menores costos y mayor velocidad para el sistema interbancario;
- ii) la implementación de operaciones de mercado abierto del banco central 24 horas al día, siete días por semana, y la reducción del riesgo de las transacciones nocturnas;
- iii) un esquema más simple para pagar intereses en divisas del banco central; y
- iv) reemplazar los roles actuales de otorgamiento de créditos y creación de dinero por parte de los bancos comerciales, con un sistema bancario más acotado, en el cual las instituciones financieras tienen una estructura de capital de apalancamiento mínimo o nulo. Una moneda digital de los bancos centrales podría mejorar la transmisión de la política monetaria a través de un impacto positivo sobre los canales de los balances y de la toma de riesgo, debido a la menor necesidad de garantías y a la mayor transparencia.

De acuerdo con Barrdear y Kumhof (2016), el menor riesgo y las menores necesidades de garantías también podrían reducir la tasa de interés real agregada, lo que podría implicar un incremento significativo en el capital y el producto.

³² En este caso, las monedas digitales creadas por los bancos centrales sólo operarían como un medio para realizar transacciones bancarias de forma más eficiente. Esto no está relacionado con una economía “sin efectivo”, puesto que el valor del efectivo para las transacciones realizadas por el público y como depósito de valor es virtualmente imposible de sustituir.

Por otro lado, permitir el acceso masivo a los balances del banco central puede plantear grandes desafíos. De acuerdo con Furche et al. (2017), el principal desafío es pasar de docenas de socios mayoristas a miles o millones de minoristas que, actuando como retail, competirían directamente con las cuentas de depósito en los bancos comerciales. En el caso de que esto ocurriera, las monedas digitales de los bancos centrales podrían llevar a la sustitución de su rol clásico, en la cima de un sistema estratificado de liquidez, por el de un minorista masivo. Puesto que los bancos comerciales dependen de manera significativa de los depósitos y de la generación de préstamos de un sistema de encaje fraccionado, la creación de monedas digitales de los bancos centrales podría tener como efecto negativo privar a los bancos e instituciones financieras de su principal fuente de fondos. Esto podría producir que los hogares y las empresas en busca de crédito terminen enfrentando más dificultades debido al término de una banca fraccionada. Adicionalmente, los especuladores tendrían acceso a información relevante sobre los puntos débiles de una institución financiera específica o del sistema en su conjunto y explotar esta información en ataques especulativos.

Por todo lo anterior, el Consejo de Estabilidad Financiera (2017) sostiene que, en el caso de que los bancos centrales creen sus propias monedas digitales, es más probable que las utilicen como un instrumento para actualizar sus sistemas de liquidación bruta en tiempo real y actualizar los mercados interbancarios, más que como una moneda digital de uso universal por el público general. Sin embargo, de acuerdo con Broadbent (2016), el carácter centralizado de los sistemas de liquidación bruta en tiempo real ya es muy eficiente e involucra a pocos intermediarios; por lo tanto, el uso de tecnologías de contabilidad distribuida y de cadena de bloques no implicaría mejoras significativas.

4.5 Dilemas y desafíos para los banqueros centrales y reguladores

Si bien las nuevas empresas de FinTech y sus desarrolladores muchas veces son considerados el opuesto exacto de los bancos centrales, que por su naturaleza son conservadores, los desafíos que plantean no son completamente nuevos y tienen que ver con cómo constituir regulaciones que permitan el surgimiento y desarrollo de innovaciones sin comprometer la estabilidad y la confianza.

A continuación, se presentan algunos de los dilemas de la banca central que presenta Furche et al. (2017) a la hora de regular los desarrollos FinTech:

Inclusión versus riesgo de decisiones no informadas: Como se mencionó anteriormente, uno de los principales beneficios potenciales de las innovaciones de FinTech, en particular para las economías emergentes, es la inclusión financiera, en la medida en que más personas pueden tener acceso a servicios financieros. Sin embargo, a pesar de que esto puede ser positivo en el caso de los productos financieros más básicos, como los sistemas de pago, puede que no lo sea para los productos que plantean riesgos financieros mayores para el cliente estándar. En este caso, el desafío de política pública es promover la educación financiera y un marco adecuado de protección financiera al consumidor.

Descentralización, elección y competencia versus eficiencia operativa, economías de escala y conocimiento del cliente: Si las innovaciones de FinTech tienen el potencial de desagregar las principales funciones de las instituciones financieras, es posible que muchas empresas relativamente pequeñas se apropien de un porcentaje de la industria financiera (descentralización). La existencia de más empresas entrega a los clientes más alternativas de servicios financieros y una mayor competencia. Sin embargo, la escala es un factor importante en el sector financiero y la existencia de muchas empresas ofreciendo el mismo servicio no siempre resulta ser eficiente. En ese sentido, las empresas existentes pueden tener una ventaja sobre las innovaciones de FinTech, que consiste en el conocimiento de sus clientes. En este caso, al mercado le corresponde resolver el punto de equilibrio entre competencia y eficiencia, y para esto, el regulador debe asegurar la igualdad de condiciones, y realizar un seguimiento del proceso de descentralización, si es que éste se produce.

Evaluación del crédito personal y privacidad: El uso de la información financiera personal es quizás uno de los temas más complejos en la era de la información. Por un lado, el acceso a esta información posibilita una mejor y más focalizada entrega de productos financieros, y disponer de registros adecuados de comportamiento financiero puede mejorar la calificación del crédito, lo que puede traducirse en beneficios para el consumidor. Sin embargo, el acceso sin restricciones para las compañías FinTech podría atentar contra la privacidad de las personas. El desafío del regulador está en definir un punto intermedio en que se permita algún tipo de acceso y uso de la información financiera por parte de las compañías FinTech, y definir las sanciones por mal uso o filtraciones.

Inclusión versus formalización: Como se mencionó anteriormente, las innovaciones de FinTech permiten a las personas acceder a servicios financieros tales como pagos o instrumentos de ahorro e inversión, que de otra forma no podrían adquirir, a pesar de calificar para dichos servicios. Sin embargo, cuando las personas confían sus recursos a entidades informales o desreguladas de FinTech, puede que estén tomando riesgos mayores a los que estarían dispuestos a tomar, por desconocimiento, por ejemplo. Asimismo, los peligros de lavado de dinero y elusión de impuestos aumentan, porque la aplicación de estas reglas es más difícil para las entidades que se mueven fuera del perímetro de regulación³³.

Como se mencionó al principio del capítulo, los desafíos que pueden ser menos propios de FinTech son aquellos relacionados con la ciberseguridad. Otro punto importante es que, debido a la naturaleza de FinTech, puede que sea necesaria la cooperación internacional entre los supervisores, tanto para aplicar las regulaciones locales como para evitar el arbitraje regulatorio.

³³ En el caso de América Latina, la mayoría de las nuevas empresas FinTech promueven soluciones digitales que operan en el sistema financiero formal.

En suma, el desafío de los bancos centrales está en alinear los avances de las empresas FinTech con los objetivos de control de la inflación y estabilidad financiera, que dependen, en última instancia, de las regulaciones establecidas por los propios bancos centrales y las autoridades financieras.

4.6 FinTech en América Latina

Por lo general, la oferta de servicios FinTech tiene algún grado de relación con el nivel de desarrollo y las necesidades de cada país. Por ejemplo, la necesidad de una mayor inclusión financiera es ciertamente más alta en las economías emergentes y, por ende, puede que los pagos, las remesas y los préstamos con FinTech tengan un mayor desarrollo que las actividades relacionadas con contabilidad distribuida.

En el caso de las economías latinoamericanas, destaca la rápida penetración de las FinTech en los últimos 4 años. Esto, debido principalmente a la desatención de ciertos segmentos de consumidores por parte del sistema financiero. En este caso, las FinTech estimulan la demanda de crédito, ofreciendo productos a menor costo, o bien, productos no ofrecidos por los principales proveedores debido a su baja rentabilidad³⁴. Destaca también el uso de los servicios FinTech en el envío de remesas, debido a sus menores costos y mayor rapidez.

4.6.1 Regulación de FinTech en el sistema financiero chileno

En el caso de Chile, las empresas FinTech coexisten con un mercado bastante amplio, diversificado y profundo de servicios financieros convencionales. En el país, destaca el rápido crecimiento del financiamiento colectivo (o *crowdfunding*³⁵), que parece haberse desarrollado a partir de su conexión con los servicios de intermediación financiera (o *factoring*³⁶).

³⁴ Como ya vimos, el desarrollo de las FinTech va de la mano con el objetivo de inclusión financiera, y con los desafíos ya vistos para las autoridades, elementos comunes compartidos por las principales economías de la región.

³⁵ Un *crowdfunding* es una cooperación colectiva que reúne a varias personas interesadas en realizar un proyecto, para lograr el financiamiento de forma colectiva. Es muy útil para personas con proyectos o *start-ups* que no califican o deciden no utilizar las alternativas tradicionales de financiamiento, como serían los bancos y entidades prestadoras de dinero. Financiar la puesta en marcha de un proyecto mediante *crowdfunding* tiene ventajas que van más allá del dinero recaudado, como por ejemplo, la posibilidad de medir el nivel de aceptación o atractivo del proyecto a través de la opinión de los cofinanciadores que se mide en la disposición a aportar para la implementación de la idea. Si se recauda el total del monto requerido, puede ser una señal muy clara de aceptación del producto o servicio en el mercado. Si no se logran recaudar los fondos solicitados, puede ser una señal de que hay que rediseñar el proyecto. Los cofinanciadores pueden recibir recompensas monetarias o en términos de futuros servicios brindados por el proyecto.

³⁶ El financiamiento colectivo en Chile es un ejemplo de los dilemas que enfrentan los reguladores financieros. La industria del financiamiento colectivo en Chile ha proliferado a pesar de que la autoridad bancaria acusó a su principal empresa de infringir la Ley de Bancos en 2012.

En la actualidad, Chile no cuenta con leyes o regulaciones específicas para las empresas FinTech, por lo que deben regirse por el marco regulatorio tradicional. Si bien ésta no es la situación óptima, al menos no desincentiva la innovación.

Cabe destacar que el esquema de regulación financiera en Chile está teniendo un importante cambio, pasando de un enfoque tradicional a una instancia de supervisión financiera integrada, la Comisión para el Mercado Financiero (CMF), que estará integrada por las entidades reguladoras de valores, seguros y bancos (Superintendencia de Valores y Seguros y Superintendencia de Bancos e Instituciones Financieras, respectivamente).

En la ley actual (n.º 21.000), la CMF tiene el mandato de resguardar la estabilidad financiera; puede promover regulaciones para la aplicación de leyes dentro de su área de competencia; y también puede proponer nuevas leyes y regulaciones consideradas necesarias para el funcionamiento de los mercados financieros al Presidente de la República, a través del Ministerio de Hacienda. Sin embargo, no es evidente cómo las características y atribuciones de la CMF podrán contribuir a superar las restricciones legales que enfrentan los reguladores existentes, en una forma más eficiente que el enfoque tradicional anterior, particularmente a la hora de enfrentar los desafíos de las innovaciones FinTech. Quizás una buena opción sería el desarrollo de una “ley FinTech” más flexible y específica, como en los casos de Singapur, Reino Unido y México.

5. Conclusiones y Discusión

El sistema blockchain es una herramienta excepcional y con gran potencial, pero, como todas las tecnologías, no es bueno ni malo en sí mismo. Podemos usar magníficas tecnologías, desde la electricidad hasta la radio pasando por internet, para fines buenos o malos. Por esto, necesitamos que se desarrolle un liderazgo capaz de aprovechar la tecnología blockchain para hacer el bien en nuestras instituciones, en organizaciones humanitarias y de la sociedad civil, en empresas, en gobiernos y en las personas que se conecten a esta vasta red. Sólo cuando estos desafíos se hayan superado se desarrollará plenamente el potencial de la tecnología blockchain como instrumento de prosperidad global y cambio positivo.

En esta misma línea, ¿es realmente deseable que todo quede registrado inmutable y permanentemente? En Europa hay tribunales que fallan a favor del “derecho al olvido” y dan curso a demandas de personas que quieren borrar su historial de internet. ¿No habría que aplicar el mismo principio a las empresas? ¿No tienen las empresas derecho a cambiar su historial, derecho al olvido? Tapscott y Tapscott (2017) sostienen que no. Como productos de la sociedad que son, las empresas tienen responsabilidades inherentes al permiso que se les ha dado para operar. Además, tienen el deber para con la sociedad de hacer pública toda la información que se refiera a sus negocios. Claro está que las empresas tienen el derecho y la obligación de guardar el secreto industrial y proteger la privacidad de sus empleados, personal y demás *stakeholders*. Pero eso es otra cosa. Aumentar la transparencia es una gran oportunidad para los empresarios de todo el mundo: oportunidad de elevar al máximo los niveles de calidad de la gestión empresarial y erigirse en referentes de la confianza, y todo eso posibilitado gracias a la adopción de la tecnología blockchain.

Otra arista importante, y que queda abierta, es analizar los riesgos y efectos de transferir tanto poder desde los intermediarios financieros tradicionales a los programadores. Es importante porque el mundo de la programación puede quizás ser aún más desigualdad en términos de acceso e información que el sistema financiero tradicional.

Otra materia que se debe tener en consideración para el futuro próximo son los efectos del desarrollo de la computación cuántica en la tecnología blockchain y en la criptografía en general ya que permitiría disminuir los costos energéticos de esta tecnología.

Con respecto a los desarrollos FinTech, los bancos centrales y los reguladores tienen la responsabilidad de estar atentos a los avances en materia de FinTech, y tienen los desafíos de mejorar las infraestructuras de pago, potenciar la ciberseguridad, adaptar las regulaciones, y utilizar y manejar nuevos datos para evaluar los riesgos micro y macrofinancieros. Por lo anterior, es probable que la irrupción de las empresas FinTech aumente la importancia de la coordinación entre el Banco Central y los demás reguladores financieros.

La tecnología está creando nuevas oportunidades para cambios en los servicios financieros masivos, en las instituciones financieras y en los bancos centrales. Las tecnologías de la información están operando este cambio porque las finanzas son en gran medida un negocio de información y de mantención de registros. En ese sentido, la tecnología de contabilidad distribuida y otros desarrollos tecnológicos abren la posibilidad de una desagregación de los servicios financieros tal que a veces llega a cuestionar la existencia misma de los bancos y otros intermediarios.

El acceso a estas tecnologías abre grandes oportunidades, no sólo para las nuevas empresas financieras y el público, sino también para los líderes de los países emergentes, que pueden ver en estos avances tecnológicos la posibilidad de impulsar el desarrollo financiero y superar un importante obstáculo al crecimiento económico inclusivo. Más aún, pueden aprovechar el mayor acceso a los servicios financieros para promover una formalización de la actividad económica y evitar el crecimiento de la economía informal. Sin embargo, para materializar esta idea, los diseñadores de políticas deben asegurarse de que no están exponiendo a las personas a mayores riesgos.

En Chile, la existencia de registros seguros de identidad, el acceso masivo a internet, una amplia oferta de servicios complementarios en red y, por sobre todo, cuentas bancarias casi universales, son señales de que es posible avanzar en la incorporación de FinTech. Esto se transforma en un desafío también para los proveedores de servicios financieros tradicionales, ya que deben adaptar sus modelos de negocio y estar preparados para compartir el mercado con otros agentes no tradicionales.

Como afirman Furche et al. (2017) hacia el final de su trabajo, *“el principal activo de un banco central hoy no es el oro que guarda en sus bóvedas, sino la confianza del público. Ser capaces de comprender la revolución FinTech y asegurar que ésta contribuya a la estabilidad económica y el bienestar de las personas es la clave para conservar esa confianza”*.

Referencias

Acuña, H. (2017). Estudio sobre Bitcoin y Tecnología Blockchain. Cuadernos CEF, ESE Business School, Universidad de Los Andes. Disponible en: <https://www.esec.cl/esec/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html>

Auer R. The Mechanics of Decentralised Trust in Bitcoin and the Blockchain, BIS Working Papers.

Banco de Pagos Internacionales (2009). Issues in the Governance of Central Banks. Reporte del Grupo de Gobernanza del Banco Central³⁷, Banco de Pagos Internacionales (mayo).

Barrdear, J. y Kumhof, M. (2016). The Macroeconomics of Central Bank Issued Digital Currencies. Working Paper 605, Bank of England.

Bernanke, B. y Gertler, M. (1995). Inside the Black Box: The Credit Channel of Monetary Policy Transmission. Journal of Economic Perspectives 9 (4): 27-48.

BIS (2018). Annual Economic Report, June.

Bravo, J.A. y Hardings J. (2018). La Tecnología Blockchain, una Revolución Modernizadora en Marcha. Working Papers CEPAL.

Brennan, B., Baccala, M. y Flynn, M. (2017). Artificial Intelligence Comes to Financial Statement Audits. CFO Newsletters, 2 de febrero. <http://ww2.cfo.com/auditing/2017/02/artificial-intelligence-audits/>.

Broadbent, B. (2016). Central Banks and Digital Currencies. Conferencia dada en London School of Economics and Political Science. 2 de marzo. <http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech886.pdf>.

Consejo de Estabilidad Financiera (2017). FinTech Credit. Financial Stability Board Report (27 de junio).

Deloitte. (2016). Developing Legal Talent: Stepping into the Future Law Firm. (febrero). <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-developing-legal-talent-2016.pdf>.

FINMA (2018). Guidelines for Enquires Regarding the Regulatory Framework for Initial Coin Offerings (ICOs).

Fondo Monetario Internacional (2016). Monetary Policy and the Rise of Nonbank Finance. Reporte de Estabilidad Financiera Global, Capítulo 2 (octubre).

³⁷ El Grupo de Gobernanza opera como un espacio para el intercambio de puntos de vista entre los gobernadores y presidentes de los bancos centrales sobre asuntos relacionados con el diseño y el funcionamiento de sus instituciones. La atención se centra en el entorno institucional y organizativo en el que los bancos centrales persiguen las políticas monetarias y financieras, y no en las políticas en sí mismas. Además, proporciona un panel de discusión para los gobernadores y presidentes que también actúa como un comité directivo para el Foro.

Furche, P., Madeira, C., Marcel, M. y Medel, C. (2017). FinTech y la Banca Central en la Encrucijada. Estudios Públicos, 148, 39-78.

Haliassos, M. (2015). Keeping Households out of Financial Trouble. En Financial Regulation, editado por Faia et al.

Levine, R. (2017). Financing Prosperity, University of California, Berkeley

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

Philippon, T. (2017). The FinTech Opportunity. Working Paper 655, Bank of International Settlements (agosto).

Raddatz, C. y Vergara, R. (2016). Macroprudential Policies: General Analysis and a Look into the Chilean Experience. Economic Policy Paper 59, Banco Central de Chile (marzo).

Raskin, M. y Yermack, D. (2016). Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. Working Paper 22238, National Bureau of Economic Research (mayo).

Tapscott, D. y Tapscott, A. (2017). The Blockchain Revolution.

Linkografía

¿Qué es una ICO?: <https://cointradors.com/es/basics/que-es-una-ico/>

¿Qué es un Crowdsale de Cryptocurrency?: <https://es.routestofinance.com/what-is-cryptocurrency-crowdsale>

¿Por qué Suiza se está convirtiendo en una “cripto nación” con un mercado floreciente de ICOs?: Opinión de Expertos: <https://es.cointelegraph.com/news/why-switzerland-is-becoming-a-crypto-nation-with-a-flourishing-ico-market-expert-take>

Autoridad financiera de Suiza publica guía para el tratamiento de las ICO: <https://www.diariobitcoin.com/index.php/2017/10/04/autoridad-financiera-de-suiza-publica-guia-para-el-tratamiento-de-las-ico/>

Autoridad financiera de Suiza regula las ICO y clasifica tres tipos de token: <https://www.criptonoticias.com/regulacion/autoridad-financiera-suiza-regula-ico-clasifica-tres-tipos/>

Autoridad financiera suiza publica directrices reguladoras específicas para las ICOs: <https://es.cointelegraph.com/news/swiss-financial-authority-releases-ico-specific-regulatory-guidelines>

El estatus legal de las ICO en 6 grandes naciones: <https://es.linkedin.com/pulse/el-estatus-legal-de-las-ico-en-6-grandes-naciones-daniel-mery>

Guía de la ICO: Oferta inicial de monedas: <http://tecnologiabitcoin.com/guias-tutoriales/guia-ico-oferta-inicial-monedas/>

ICO, Explicado: <https://es.cointelegraph.com/explained/ico-explained>

Suiza aprueba las directrices para las ICOs: <https://criptotendencia.com/2018/02/19/suiza-aprueba-las-directrices-para-las-icos/>

Suiza elabora directrices ICO: <https://www.crypto-economy.net/suiza-elabora-directrices-ico/>

Suiza pone normas a las operaciones empresariales con criptomonedas: https://elpais.com/economia/2018/02/16/actualidad/1518785688_172151.html

Suiza quiere aplicar normativas ya existentes para operar con criptomonedas: <https://www.cronista.com/financiertimes/Suiza-quiere-aplicar-normativas-ya-existentes-para-operar-con-criptomonedas-20180221-0014.html>

Suiza regulará las ICO con las leyes del país para evitar estafas y blanqueo de capitales: <https://hardwaresfera.com/suiza-regulara-las-ico-las-leyes-del-pais-evitar-estafas-blanqueo-capitales/>

Suiza vinculará los procesos de las ICO con la legislación vigente en el país: <https://www.cryptonoticias.com/regulacion/suiza-vinculara-procesos-ico-legislacion-vigente-pais/>