REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 7 NÚM. 1 (2018) • PÁGS. 79-105 • DOI 10.5354/0719-2584.2018.48515
RECIBIDO: 5/3/2018 • APROBADO: 6/6/2018 • PUBLICADO: 30/6/2018

DOCTRINA

Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal

Risks of criminal actions with virtual currencies: New challenges for criminal law

Francisco Bedecarratz Scholz

Universidad Autónoma de Chile

RESUMEN Las monedas virtuales son un fenómeno nuevo que está impactando crecientemente el tráfico jurídico nacional e internacional. Su acelerada masificación requiere la creación de un modelo preventivo para impedir su aprovechamiento en actividades delictivas y proteger a sus usuarios. Este trabajo examina la tecnología de las monedas virtuales y sus características relevantes desde el punto de vista del derecho penal y de la criminología. El análisis se centra en el aumento del riesgo que ocasionan en relación con delitos de alta complejidad, enfocado particularmente en el lavado de activos. El artículo critica la aplicación de modelos convencionales para su regulación y concluye con una propuesta regulatoria preventiva acorde a la naturaleza y *modus operandi* de esta nueva tecnología.

PALABRAS CLAVE Monedas virtuales, criptomonedas, *RegTech*, *blockchain*, lavado de activos.

ABSTRACT Virtual currencies are a new phenomenon that is increasingly affecting both national and international legal traffic. Their rapid spread requires the conception of a prevention model in order to deter its utilization in criminal activities and protect the users. This paper examines the technology of virtual currencies and studies its relevant characteristics from the standpoint of criminal law and criminology. The analysis emphasizes the risk increase it causes regarding highly complex criminal offenses, particularly money laundering. The paper criticizes the usage of conventional models for its regulation, and concludes with a new preventive regulatory approach that is consistent with the nature and *modus operandi* of this new technology.

KEYWORDS Virtual currencies, cryptocurrencies, RegTech, blockchain, money laundering.

Introducción

La creación del protocolo Bitcoin por Satoshi Nakamoto en el año 2008 (Nakamoto, 2008) inició a nivel mundial una progresiva expansión de las monedas virtuales. La actual masificación en el uso de estos instrumentos ha generado una intensa discusión sobre su impacto en la sociedad y la reacción adecuada que el derecho debe presentar al mismo.

En la ciencia penal, el debate se ha centrado en los riesgos delictivos que presentan las monedas virtuales, así como las posibilidades de regulación y de sanción que ofrecen los ordenamientos jurídicos actuales. Sin embargo, las características inherentes a las monedas virtuales generan serias dudas sobre la aptitud de las instituciones vigentes de *lege lata* para controlar y sancionar efectivamente su mal uso. Además, no existe consenso sobre la estrategia específica que mejor se adecúa a la naturaleza de las criptomonedas, esto es, si es preferible un enfoque penal o regulatorio para enfrentar el fenómeno.

Este trabajo tiene por objeto explicar la naturaleza, funcionamiento y riesgo criminógeno que presentan las monedas virtuales, así como valorar las respuestas que nuestro ordenamiento jurídico puede ofrecer, con el fin de sancionar su uso criminal. Basado en este análisis, entrega finalmente una propuesta regulatoria nueva para enfrentar de mejor manera este fenómeno. El objeto específico del estudio es la tecnología *blockchain* empleada por el Bitcoin, la moneda virtual más antigua y difundida hasta la fecha.[1]

Aspectos generales de las monedas virtuales

El análisis de la relevancia jurídico-penal de las monedas virtuales hace necesario inspeccionar sus aspectos esenciales. Con dicho objeto, el presente capítulo ofrecerá una definición de las monedas virtuales y resumirá brevemente su funcionamiento y características.

Hacia un concepto de moneda virtual

Las «monedas virtuales» han sido definidas por la Autoridad Bancaria Europea como «una representación digital de valor, que no es emitida por un banco central o una autoridad pública, ni necesariamente conectada a un dinero fiduciario, pero es aceptada por personas naturales o jurídicas como medio de pago y puede ser transferida,

1. Además del Bitcoin, existen otros sistemas de monedas virtuales que presentan características o funciones especiales, como Ripple o Ethereum. Por los motivos ya expuestos, este trabajo empleará como caso de estudio el Bitcoin.

almacenada o intercambiada electrónicamente».[2] Por su parte, el Banco Central Europeo las define como una «representación digital de valor, no emitida por ninguna autoridad bancaria central, institución de crédito o emisor de dinero electrónico que, en ciertas ocasiones, puede ser utilizada como una alternativa al dinero».[3]

Los conceptos propuestos por la Autoridad Bancaria Europea y por el Banco Central Europeo comparan las monedas virtuales con el dinero fiduciario común, también denominado «dinero fíat». Este último se define como cualquier moneda legal diseñada o emitida por una autoridad central,[4] la cual se basa en la confianza depositada en la autoridad central que la emite.[5] En concreto, los conceptos apuntan a que poseen una naturaleza puramente digital y no física, no cuentan con el respaldo de una autoridad central y constituyen una alternativa al dinero. Sin embargo, si bien el término «moneda virtual», en su sentido natural y obvio, sugiere que estarían en una misma categoría con las monedas fiduciarias —por tanto comparables—, constituyen en realidad instrumentos de naturalezas diferentes y que pertenecen, por consiguiente, a órdenes distintos.

Las definiciones son criticables en concreto, pues parten de la base de que las monedas virtuales comparten las características propias de una moneda, en cuanto a que serían aceptadas como un medio de pago o de cambio y contarían, por lo tanto, con poder liberatorio.[6] Sin embargo, ello no es tal, pues la actual masificación de las monedas virtuales no ha alcanzado a producir una aceptación de las mismas en el sistema económico, lo cual implica que carecen de ese poder. Aún falta una penetración en la sociedad de estos instrumentos que produzca su general aceptación por las personas. A su vez, la carencia de respaldo de las monedas virtuales por parte de un gobierno central, unido al creciente uso que se les da como alternativa de inversión o especulación —cerca del 70% de los usuarios (Cifuentes Hurtado, 2017: 6)—, traen como consecuencia una alta volatilidad que distorsiona su utilidad como unidad de cuenta.

Pareciera más acertado reconocer a las monedas virtuales como una especie de

2. Autoridad Bancaria Europea, «EBA opinion on «virtual currencies»», 4 de julio de 2014, p. 11, disponible en http://bit.ly/2t8C2Hq.

3. Banco Central Europeo, «Virtual currency schemes: A further analysis», febrero de 2015, p. 25, disponible en http://bit.ly/2lez4Oh.

4. Banco Central Europeo, «Virtual currency schemes», octubre de 2012, p. 9, disponible en http://bit.ly/2t6J53r.

5. El dinero electrónico (*e-money*) es una representación digital del dinero fiduciario, que tiene por tanto una naturaleza distinta a la de las monedas virtuales. En otras palabras, el dinero electrónico es un mecanismo digital de transferencia de dinero fiduciario (Arias Acuña y Sánchez Pullas, 2016: 176).

6. Según la teoría monetaria clásica, dinero es cualquier bien que actúe como medio de cambio, unidad de cuenta y almacén de valor (Harris, 1993: 15). Sobre la historia del dinero en relación con las monedas virtuales, véase Trautman y Harrell (2017: 1.043 y ss.).

bien incorporal *sui generis* que como una moneda, las cuales pueden ser empleadas como un *commodity* y ser objeto de transacciones e inversiones, como ha ido ocurriendo hasta la actualidad. Mientras estas herramientas no sean depositarias de una aceptación generalizada en la sociedad como medio de pago, no puede calificárselas como moneda, al contrario de lo que postulan las definiciones del Banco Central Europeo o la Autoridad Bancaria Europea.

Comúnmente se usa como sinónimo de «monedas virtuales» el término «criptomonedas». Este último concepto las vincula a la criptografía, tecnología de cifrado que constituye la arquitectura de su funcionamiento y garantía de su valor, en contraposición al dinero fiduciario común que se sustenta en la confianza. Cabe aclarar que todos los tipos de monedas virtuales que utilizan el protocolo Bitcoin emplean el método criptografía, representada por la tecnología *blockchain*.

Recepción normativa

Dejando atrás las definiciones ontológicas y entrando en materia normativa, las monedas virtuales no cuentan con un reconocimiento legal o reglamentario en Chile, pues el concepto y sus sinónimos están absolutamente ausentes de la legislación nacional.[7] En atención a la reciente masificación de estos instrumentos, la literatura jurídica nacional tampoco exhibe una especial frondosidad en la materia, solo existen pocos estudios acerca de su relevancia jurídica. El silencio jurídico reinante en Chile sobre esta materia contrasta con el panorama en el contexto internacional.

En Alemania, el Legislador no ha especificado normativamente lo que debe entenderse por moneda virtual. Sin embargo, la Autoridad Federal de Supervisión Financiera (*Bundesanstalt für Finanzdienstleistungsaufsicht*, BAFIN) ha clasificado a las monedas virtuales como una clase de instrumentos financieros según el párrafo 1, inciso undécimo, número 7, alternativa segunda de la Ley Bancaria alemana (*Kreditwesengesetz*), y las define específicamente como «unidades de cuenta» (*Rechnungseinheiten*).[8] En este sentido, son comparables al carácter que asumen las divisas en el ordenamiento jurídico alemán, así como también otras unidades que funcionan como medios de pago o monedas privadas en virtud de una convención entre varias partes.[9] Cabe destacar que la definición realizada por la BAFIN tiene efectos jurídicos vinculantes, pero circunscritos únicamente al campo regulatorio financiero.

7. Al 31 de mayo de 2018, no existen proyectos de ley ingresados al Congreso Nacional que contengan las palabras «monedas virtuales», «criptomonedas» o «altcoins».

8. Una unidad de cuenta es un operando o magnitud definido artificialmente, en función del cual se establece el valor o precio de bienes o servicios. Consúltese también a Harris (1993: 20 y ss.).

9. Jens Münzer, «Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer», BAFIN, 19 de diciembre de 2013, disponible en http://bit.ly/2JSOqpy. La toma de posición de la BAFIN fue hecha a propósito del Bitcoin, pero es interpretada como válida para todo tipo de monedas virtuales.

Por otra parte, la BAFIN ha establecido expresamente que las monedas virtuales no son reconocidas como medios de pago legales y que tampoco son divisas propiamente tales. Este limitado e incluso contradictorio reconocimiento del ente regulador alemán tiene como objeto obligar a aquellos operadores que realizan regularmente transacciones con monedas virtuales a obtener autorización para efectuar la actividad, al someterlos al mismo tiempo a cierto grado de supervisión por parte de los entes reguladores financieros alemanes. Además, tiene por fin sujetar el comercio de Bitcoin y análogos al sistema tributario alemán, además de obtener el pago de impuestos a la renta de aquéllos que transan regularmente y obtienen utilidades de estos instrumentos. Sin embargo, se ha evitado expresamente reconocerlos como un medio de pago, lo que de esta forma previene su masificación.

Distinta es la evolución que ha experimentado el concepto de monedas virtuales en el ordenamiento jurídico japonés. La Ley de Servicios de Pago (Ley 59 del 24 de junio de 2009) fue modificada con efecto al 1 de abril de 2017, en orden a reconocer a las monedas virtuales como parte integrante del sistema bancario y regulatorio nipón. Dentro de los cambios efectuados en la ley, se introdujo en su artículo 2 numeral quinto el concepto de lo que debe entenderse como «moneda virtual». Se les define como «valores de propiedad» que pueden ser comprados, vendidos, intercambiados y, especialmente, usados como una «forma o medio de pago», y pueden ser transferidos a través de un sistema electrónico de procesamiento de datos. Sin embargo, la definición omite declararlas como una moneda legalmente reconocida. En este sentido, las monedas virtuales constituyen en realidad un activo susceptible de ser objeto de operaciones comerciales, pero no una moneda. Junto a este reconocimiento, se estableció en sus nuevos artículos 63.2 a 63.22 una serie de regulaciones para los proveedores de servicios relacionados con monedas virtuales, los cuales establecen el deber de registrarse ante el ministerio respectivo, de someterse a supervisión, reportar periódicamente a los reguladores, implementar medidas de protección para los usuarios y más.

En paralelo a esta reforma, la Ley para la Prevención de Transferencia de Ganancias Delictuales (Ley 22 del año 2007), parte fundamental del sistema de prevención de lavado de activos de Japón, también fue modificada. Dentro de los cambios se dispuso la obligación de que las casas de cambio de monedas virtuales implementen políticas de identificación de clientes nuevos (*know your customer*), mantengan registros de sus transacciones y reporten a las autoridades sobre cualquier operación sospechosa originada en el marco de comercio de monedas virtuales. Es decir, se asociaron a los proveedores de servicios de monedas virtuales similares deberes de identificación, monitoreo y reporte que los exigidos a otras instituciones financieras, en el marco de la prevención de operaciones de blanqueo de activos. Cabe detenerse sobre este último punto.

La decisión del Legislador japonés de obligar a los operarios de los sistemas de

monedas virtuales a cumplir tareas de prevención de lavado de activos no es una particularidad del ordenamiento jurídico nipón, sino que es la solución actualmente dominante a nivel mundial. Volviendo a Europa, esta propuesta también ha sido impulsada por la Comisión Europea, poder ejecutivo y de iniciativa legislativa en la Unión Europea, como parte integrante de la Cuarta Directiva de Lavado de Activos.[10]

Sin embargo, la conveniencia de esta vía regulatoria debe estudiarse en estrecha relación con las características de las monedas virtuales. El desarrollo de políticas de prevención efectivas requiere una comprensión acabada de la forma de operación de estos sistemas. Para ello, se expondrá a continuación una perspectiva general de su funcionamiento basada en el sistema Bitcoin, el cual emplea una tecnología compartida por la gran mayoría de monedas virtuales actualmente en el mercado.[11]

Perspectiva general sobre el funcionamiento del sistema Bitcoin

El Bitcoin fue ideado con el fin de ser una moneda sustituta del dinero fiduciario común, de carácter no estatal, de cantidad limitada y administrada a través de una red computacional distribuida. Esta criptomoneda tiene por objeto satisfacer mediante tecnologías de la información numerosas necesidades legítimas del mercado globalizado, como bajo o nulo costo directo de transferencias, rapidez de las operaciones, facilidad de traspasos internacionales, protección de privacidad y salvaguarda frente al fraude (Rogojanu y Badea, 2014: 109-110). La forma como ello se verifica en los hechos se puede explicar mediante las diferencias de su funcionamiento en relación con el dinero fiduciario común.

A diferencia del dinero común, que puede ser creado en forma ilimitada mediante nuevas emisiones —lo cual va unido al riesgo de inflación—, nuevos Bitcoin son creados a través de un procedimiento matemático ejecutado por la red de usuarios. Al efecto, los participantes deben resolver, a través de programas computacionales, problemas criptográficos de complejidad creciente, proceso que se denomina minería o *mining*. La resolución exitosa de uno de estos problemas es recompensada con nuevos Bitcoin. La progresiva complejidad de los algoritmos implica que la generación de las monedas sea cada vez más lenta y costosa en recursos computacionales y electricidad. Solo puede crearse un número limitado de Bitcoin, por lo que puede existir un máximo de aproximadamente 21 millones de monedas. Para facilitar su comerciabilidad, los Bitcoin son fraccionables en unidades más pequeñas.

10. «Comunicación de la Comisión al Parlamento Europeo y al Consejo: Plan de acción para intensificar la lucha contra la financiación del terrorismo», Comisión Europea, 2 de febrero de 2016, disponible en http://bit.ly/2JPwxI2.

11. Un resumen del funcionamiento de la tecnología *blockchain* y de las operaciones en el sistema Bitcoin puede encontrarse en Acuña Sáez (2017: 16 y ss.).

Los usuarios toman parte en transacciones de Bitcoin a través de programas —también denominados «clientes»— instalados directamente en sus equipos computacionales (computadores, *tablets*, *smartphones*, etcétera), sin que exista una instancia central que ejecute, autorice o controle las transacciones. Cada usuario interviene directamente y en igualdad de condiciones respecto del resto, y todo el sistema funciona en base al principio de red entre pares o *peer to peer*.

Los Bitcoin son adjudicados o adscritos a direcciones o cuentas, las cuales son una serie de caracteres alfanuméricos generados por el cliente del usuario respectivo y que funcionan como destino de la moneda. Dado que es posible poseer una cantidad ilimitada de direcciones, el usuario las administra con su cliente mediante monederos o *wallets*. Junto con las direcciones, los monederos contienen también un par de claves, compuestas por una pública y otra privada, que sirven para autentificar las transacciones de Bitcoin entre los usuarios de la red.

Una transacción de Bitcoin se perfecciona mediante la transferencia directa desde la dirección del usuario oferente hacia la dirección del usuario aceptante. La transferencia propiamente tal consiste en un mensaje de que el Bitcoin debe ser asignado a otra dirección. Con el objeto de asegurar en una primera instancia que solo el dueño de la dirección pueda disponer del Bitcoin destinado a la misma, la transacción debe ser firmada digitalmente con la clave privada perteneciente al monedero respectivo.

Dado que en este sistema está ausente una contraparte central que autorice y certifique las transacciones, la validación la ejecutan otros usuarios de la red mediante un procedimiento de consenso multilateral denominado prueba de trabajo o *proof of work*. Los participantes emprenden la resolución de un problema criptográfico asociado a la operación, logrado lo cual certifican la validez de la transferencia.[12] Esta labor —costosa en recursos computacionales y consumo eléctrico— es la minería ya referida anteriormente, y que es recompensada con una nueva emisión de Bitcoin para el minero.

Respecto de cada Bitcoin se guarda una historia de esta y anteriores transferencias en un registro público compartido denominado *blockchain* o cadena de bloques. La forma como ello ocurre es empaquetando cada transferencia en bloques y luego verificando su autenticidad por los mineros. Una vez validados, los bloques o paquetes conjuntos de transacciones son incluidos en la cadena y distribuidos a los participantes de la red Bitcoin (Acuña Sáez, 2017: 23). Una copia del *blockchain* es almacenada en cada computador de la red o «nodo». Estos computadores son sincronizados periódicamente con el fin de asegurar que todos compartan una idéntica base de datos (Wright y De Filippi, 2015: 7).

En este archivo se deja constancia de la historia de transacciones Bitcoin que han

12. La certificación dice relación principalmente con que no se haya dispuesto dos veces de la misma moneda (Nakamoto, 2008).

sido confirmadas como legítimas por medio del proceso de minería. A través del análisis del *blockchain* es posible elucidar el monto de Bitcoin que fueron transferidas, la dirección desde la cual fueron emitidas, la dirección a la cual llegaron y, además, el momento exacto en que ello ocurrió. Esta marca de tiempo es fundamental para conformar el orden de la cadena, con los bloques más antiguos en una posición anterior a los más nuevos, lo que soluciona así el problema de doble gasto (Acuña Sáez, 2017: 16), es decir, que el mismo usuario fraudulentamente disponga dos veces de la misma moneda. Cabe destacar que en el *blockchain* no queda registro alguno de la identidad de los usuarios que hicieron la transferencia, sino que solo de la dirección emisora y destinataria de la misma.

Además de la minería y de las transferencias ya descritas, los Bitcoin pueden ser adquiridos contratando con empresas que operen como casas de cambio de monedas virtuales.[13] Las personas pueden comprar o cambiar Bitcoin pagando con moneda de curso legal, con lo cual se conecta el sistema de moneda virtual con el sistema monetario regulado. Además, el mercado ha hecho surgir empresas que prestan servicios de pago basados en Bitcoin. Estas instituciones aceptan pagos en monedas virtuales a nombre de empresas proveedoras y prestadoras de servicios, a las cuales transfieren luego el importe en moneda de curso legal a la empresa, todo lo cual realizan a cambio de un porcentaje de la transferencia por concepto de comisión.[14]

El funcionamiento descrito grafica el particular esquema de operación de las monedas virtuales, el cual no cuenta con paralelos en el sistema financiero tradicional. De esta descripción es posible identificar características relevantes desde el punto de vista del derecho penal y de la criminología, las cuales son esenciales como factores criminógenos y también para efectos de persecución penal. Estas características se expondrán en el capítulo siguiente.

Características penalmente relevantes de los sistemas de monedas virtuales

De la estructura y funcionamiento de las monedas virtuales se sintetizan sobre todo cuatro características penalmente relevantes: se puede catalogar como un sistema no estatal, distribuido, transfronterizo y pseudoanónimo.

No estatal

Una de las características básicas del sistema de monedas virtuales es que posee plena autonomía e independencia de las instituciones estatales. Desde su origen, la gene-

13. En Chile, por ejemplo, operan Buda.com (antiguamente SurBTC), https://www.buda.com; ChileBit.net, https://chilebit.net; TradeBTC, https://tradebtc.cl; y Yaykuy, https://www.yaykuy.cl.

14. Por ejemplo, en Bitcoins.com, https://enbitcoins.com, actualmente operativo en Argentina, Brasil, Colombia, México y Venezuela.

ración de nuevas monedas en el sistema Bitcoin es regida por su propio protocolo, a cargo de los usuarios mediante el proceso de minería. Las transferencias se efectúan a través del sistema de pares directamente entre los usuarios, sin pasar por un ente regulado por el Estado como, por ejemplo, un banco. De igual modo, la certificación de las transferencias mediante el mecanismo de prueba de trabajo se efectúa por medio de los mismos usuarios. Dicha certificación dice relación solo con las características esenciales de la transferencia (monto, origen, destino y tiempo de transferencia) y no se extiende a ningún otro criterio o parámetro de naturaleza legal o reglamentaria.

De esta forma, la creación, transferencia y control de las monedas virtuales se efectúa con total independencia del Estado en cualquiera de sus formas o expresiones: bancos centrales, instituciones financieras reguladas o sistemas controladores o reguladores. En consecuencia, le está impedido al Estado determinar la cantidad de monedas virtuales emitidas al mercado, controlar las transferencias o implementar políticas preventivas de delitos a sus usuarios, por lo que en la actualidad tiene muy limitadas posibilidades de intervenir en estos sistemas.

Distribuido

Estrechamente vinculado con el carácter no estatal del esquema, tampoco existe un ente central que cree, administre o controle a las monedas virtuales. El funcionamiento del sistema se encuentra dispuesto por el protocolo respectivo y es ejecutado por los elementos que lo integran. El sistema es generado, muta y se perpetúa de forma enteramente autorreferencial.

En cuanto al cumplimiento de estas funciones, cada participante del sistema es al mismo tiempo un nodo del mismo, que forma una red que participa en igualdad de condiciones con los demás, en base al principio *peer to peer*. En este sentido, los nodos cumplen en forma compartida las tareas necesarias para el funcionamiento del sistema mediante una base de datos compartida y software automatizado (Wright y De Filippi, 2015: 19), con exclusión de cualquier ente central. Cabe destacar que la red tampoco es descentralizada, pues dicho sistema supondría un ente central que delega o traspasa funciones en nodos subordinados. Dado que no existen participantes supra ni subordinados, la red constituye en realidad una estructura distribuida (Acuña Sáez, 2017: 42) que atribuye (certificación o *proof of work, mining*) o incluso fracciona (almacenaje del registro o *blockchain*) las funciones entre sus distintos miembros (FATF, 2015b: 39).

Esta característica tiene importantes consecuencias para las estrategias regulatorias, persecutorias y punitivas. En primer lugar, cualquier tipo de enfoque regulatorio tiene que hacerse cargo de la realidad de que no existe un sujeto obligado único. No existe un nodo central que funcione como cuello de botella y al cual puedan imponérsele obligaciones regulatorias, como sí sucede con bancos e instituciones finan-

cieras. Desde un punto de vista de persecución penal, el análisis de una transferencia debe hacerse cargo de los numerosos integrantes que la conforman —desde el «minero» que creó el Bitcoin, el tradente, el adquirente y hasta aquel que haya certificado el traspaso—. Esta distribución y fraccionamiento de funciones presenta por último relevancia en materia penal sustantiva, pues el análisis de eventuales delitos debe identificar los aportes en la ejecución de cada uno de los intervinientes en la transferencia, para luego enfrentarse al problema de calificación de los aportes respectivos como formas específicas de autoría o de participación.

Como corolario de las dos características analizadas hasta el momento, cabe hacer la mención que los sistemas de monedas virtuales se inscriben en una tendencia mundial más amplia, la cual es la economía colaborativa. Este constituye un concepto amplio que incluye sistemas económicos basados en tecnologías de la comunicación, en los cuales se propende a compartir el consumo de bienes y servicios a través de plataformas en línea (Hamari, Sjöklint y Ukkonen, 2015). Un elemento en común es que estos sistemas se apoyan en la colaboración de los usuarios y fungen como estructuras paralelas a los sistemas creados o regulados por los Estados. De esta manera, la labor de los entes reguladores tiene como primer desafío individualizar los intervinientes susceptibles de ser regulados, además de determinar las herramientas adecuadas para afrontar un sistema de estas características.

Transfronterizo

Uno de los factores que impulsó la masificación de las monedas virtuales es la necesidad de un intercambio mundial facilitado por herramientas de pago transnacionales y al margen de los actores tradicionales de los circuitos monetarios (Acuña Sáez, 2017: 2). El sistema Bitcoin permite a sus usuarios efectuar operaciones internacionales sin limitaciones transfiriendo libremente a estas monedas a través de la plataforma a cualquier parte del globo.

La absoluta falta de controles para este tipo de operaciones permite, por una parte, el libre flujo de capitales alrededor del mundo, lo que facilita el comercio e intercambio internacional. Sin embargo, esta misma libertad puede ser aprovechada para mover activos provenientes de o destinados a operaciones ilícitas —como el financiamiento de operaciones terroristas—, que en un sistema convencional son filtrados por los actores tradicionales de intercambios monetarios.

Por otra parte, se dificulta la labor de organismos investigadores que intenten identificar el origen, ruta y destino de estos capitales, pues obligan al observador a considerar jurisdicciones, idiomas y situaciones geográficas ajenas a su competencia. Ello genera una dificultad técnica considerable para los entes persecutores, que debe ser solventada mediante la colaboración de personal especializado en competencias muy específicas.

Pseudoanónimo

Finalmente, una de las características más relevantes es el pseudoanonimato de los usuarios de monedas virtuales. El protocolo Bitcoin no almacena los datos de identificación de los participantes, ni tampoco genera registros históricos de las transacciones asociados a las identidades reales de los usuarios (FATF, 2015b: 32). Los traspasos y transferencias de monedas virtuales no requieren la identidad de los sujetos que emiten o reciben las monedas. Si bien es cierto que existe en el *blockchain* un registro de las direcciones de origen y destino de todas las transferencias de que ha sido objeto el Bitcoin de que se trate, cabe aclarar que lo consignado son las direcciones o cuentas, compuestas por un conjunto de caracteres alfanuméricos. Estas direcciones no están asociadas a un nombre ni están vinculadas a la identidad de los sujetos que las poseen en el mundo real. Constituyen simples identificadores generados *ad hoc* y en forma aleatoria.

Con el objeto de lograr derechamente el anonimato de los usuarios que así lo deseen, existen ciertas empresas que proveen servicios de mezclado o *mixing*. La principal función que tienen es encubrir el origen de los Bitcoin para hacer indistinguible al propietario de los mismos. Con dicho fin, los usuarios generan una nueva dirección y se la comunican al prestador de servicios, a quienes además transfieren los Bitcoin cuyo origen quieren ocultar. Acto seguido, el prestador de servicios transfiere a la nueva dirección del usuario el mismo importe de Bitcoin proveniente de un tercero. Ello ocurre no una, sino varias veces y en forma aleatoria. El efecto concreto es registrar en el *blockchain* transferencias de señuelo entre usuarios que no tienen relación previa entre sí, que dificultan el esclarecimiento del verdadero origen y destino de las monedas.[15]

Este efecto puede ser intensificado aún más mediante el uso de redes destinadas específicamente para lograr el anonimato. Una de ellas es el sistema Tor (acrónimo de The Onion Router), el cual consiste en una red de computadores que oculta la verdadera dirección IP[16] y con ello la identidad de los usuarios del sistema, a través de la redirección de las comunicaciones mediante múltiples computadoras alrededor del mundo, que enmascara además en varias capas de encriptado (FATF, 2015b: 28-29).[17] El sistema Bitcoin puede ser operado sin problemas por los usuarios en este tipo de redes. Por lo tanto, a la imposibilidad de asociar las direcciones de los Bitcoin a perso-

15. Este tipo de sitios tienen existencia relativamente efímera, debido a presiones de organismos estatales que los acusan de facilitar operaciones de lavado de activos.

16. La dirección IP (*internet protocol address*) es el numero identificador asignado a cada equipo conectado a una red. Tiene como funciones identificar al equipo y proporcionar su ubicación en la red.

17. Tor es solo uno de los sistemas utilizados en la comúnmente denominada «red oscura» o *deep web*, con el objeto de acceder a su contenido disimulando al mismo tiempo la identidad del usuario. Otros sistemas pueden ser I2P o FreeNet, entre otras.

nas determinadas, se suma el hecho de que las mismas direcciones son imposibles de vincular a una computadora específica, pues la dirección IP que identifica el equipo del cual se originó la transacción muta constantemente o es encriptada.

Riesgos delictivos

Es necesario aclarar que la creación, posesión, uso o transferencia de monedas virtuales son conductas lícitas conforme al ordenamiento jurídico penal chileno, puesto que no satisfacen ningún tipo penal de los contemplados en la ley. No obstante, las características descritas confieren a criminales un gran potencial para su uso en actividades delictivas, pues permiten disimularlas de forma más efectiva y por tanto lograr un agotamiento más seguro del delito (FATF, 2014: 9 y ss.).

En consonancia con lo anterior, las monedas virtuales han sido frecuentemente vinculadas a la comisión de variadas actividades delictivas, como ataques a empresas y extorsiones corporativas, amenazas condicionales, defraudaciones en general, comercio de pasaportes y de identificaciones falsas, tráfico de armas, pornografía y explotación infantil, así como tráfico de drogas (Trautman y Harrell, 2017: 1.087).[18]

Con todo, el Grupo de Acción Financiera contra el Blanqueo de Capitales (FATF, por sus siglas en inglés) ha analizado en una serie de publicaciones los riesgos delictivos que presentan las monedas virtuales, especialmente en relación con la prevención del lavado de dinero (*anti money laundering*) y del financiamiento del terrorismo (*countering the financing of terrorism*).[19] Siguiendo el enfoque dado por la FATF, a continuación se analizará el aumento de riesgo en relación con estos ilícitos, a los cuales se agregarán los delitos informáticos.

Delitos informáticos, Ley 19.223

El uso de monedas virtuales propiamente tal no configura una conducta punible en la forma de un delito informático de los sancionados en la Ley 19.223,[20] pues no encuadra en ninguna de las figuras típicas contempladas en la norma. Sin embargo, es posible observar el empleo de monedas virtuales como un importante accesorio en

18. Históricamente, la extinta Silk Road fue un ejemplo de plataforma basada en Bitcoin, destinada a la adquisición de bienes y servicios de comercialización ilegal (Werbach, 2017: 4). Véase el caso *United States con Ulbricht,* 31 F. Supp. 3d 540, 569, SDNY 2014.

19. Al efecto, la FATF publicó durante 2014 un reporte denominado «FATF report, virtual currencies, key definitions and potential AML/CFT risks» (FATF, 2014). En el año 2015, la publicó una guía denominada «Guidance for a risk-based approach to virtual currencies» (FATF, 2015b). Ambos documentos proponen un modelo basado en el riesgo con el fin de identificar y prevenir delitos que involucren monedas virtuales, al describir medidas regulatorias para limitar su potencial delictivo.

20. En relación con la clasificación y análisis dogmático de los delitos de la Ley 19.223, véase a Huerta Miranda y Líbano Manzur (1996: 123 y ss.) y a Magliona Markovicth y López Medel (1999: 138 y ss.).

la comisión del delito de sabotaje informático, tipificado en sus diversas modalidades en los artículos 1 y 3 de la ley citada.

Esta relación funcional entre el sabotaje informático y las monedas virtuales fue evidenciada por el ataque generado por el troyano «WannaCry», ocurrido en los meses de abril y mayo de 2017. El ataque consistió en la infección a nivel mundial de sistemas informáticos a través de un virus del tipo *ransomware*,[21] que restringía el acceso a equipos informáticos —y consiguientemente a toda la información contenida en ellos— y que ofrecía remover esta restricción a cambio de un rescate de U$300, los cuales debían ser pagados en Bitcoin. Conjuntamente se amenazaba a la víctima con la eliminación irreversible de la información contenida en el equipo secuestrado en caso de no pago.

Como regla general, la infección de un sistema informático con un troyano del tipo *ransomware* verifica una serie de figuras penales que están en relación de concurso real o material entre sí. Ello también ocurrió en el caso del virus «WannaCry»: dado que el troyano procuró acceso indebido al sistema, se configuró el delito de espionaje informático contemplado en el artículo 2 de la Ley 19.223. Mediante el bloqueo de los equipos se impidió a las víctimas su uso, por lo que se cometió el delito de atentado contra el funcionamiento de un sistema informático contemplado en el artículo 1, inciso primero, segunda parte de la Ley. La eliminación de los archivos configura, asimismo, el delito de atentado contra los datos contenidos en un sistema informático, tipificado en el artículo 3.[22] Además, la amenaza de eliminación de los datos almacenados en el equipo en caso del no pago configura por sí sola el delito de amenaza condicional sancionado en el artículo 296 números 1 y 2 del Código Penal, por lo que se opta entre uno y otro numeral según si el hechor obtuvo o no el pago del rescate por la víctima.

En caso de que sea un tercero (doloso) quien ponga a disposición sus cuentas Bitcoin para que se efectúe el pago de los delitos, ello puede ser sancionado por la vía del cómplice según el artículo 16 del Código Penal, pues constituye una facilitación para la ejecución del hecho (Politoff Lifschitz, Matus Acuña y Ramírez Guzmán, 2016: 430). En caso de que la asistencia sea posterior al hecho, ello puede ser sancionado por la vía del encubrimiento en virtud del artículo 17 números 1 y 2 del Código Penal.

En suma, las criptomonedas son especialmente propicias para lograr el agota-

21. Neologismo proveniente de una contracción de las palabras en inglés *ransom* (rescate) y software. Son programas informáticos dañinos que bloquean un equipo o parte de sus funciones, mientras exigen el pago de un rescate al usuario para recuperarlo.

22. Esta conducta configura además el delito de daños contemplado en el artículo 487 en relación con el artículo 484, ambos del Código Penal. Sin embargo, en relación con la destrucción de la información —no así del equipo físico— se prefiere la aplicación del artículo 3 de la Ley 19.223, dado que está en situación de especialidad en relación con las normas del Código Penal.

miento de estos delitos, pues proporcionan alternativas de pago para el rescate de equipos de computación bloqueados por virus del tipo *ransomware*. En efecto, gracias a las características pseudoanónimas del Bitcoin, los hechores del ataque ocasionado por el virus «WannaCry» pudieron percibir los rescates exigidos a las víctimas, lo que dificultó enormemente las tareas investigativas acerca del destino de éstos y disminuyó así el riesgo de ser detectados.

Financiamiento del terrorismo, artículo 8 de la Ley 18.314

El delito de financiamiento del terrorismo contemplado en el artículo 8 de la Ley 18.314 —introducido por la Ley 19.906 del 13 de noviembre de 2003— sanciona los casos en que se soliciten, recauden o provean fondos para ser utilizados en operaciones terroristas. En este tipo de delitos, las monedas virtuales también pueden generar un efecto facilitador o incluso criminógeno, fenómeno cuya comprensión exige graficar los métodos para el financiamiento del terrorismo.

Si bien es cierto que los costos operacionales directos de acciones terroristas como las perpetradas en Madrid en 2004 o en Londres en 2005 son relativamente modestos (FATF, 2008: 7), los gastos generales que conlleva el reclutamiento de nuevos miembros, instrucción de combatientes, creación de la estructura organizacional y manutención de los miembros —el conocido *overhead*— pueden ser cuantiosos (Sieber y Vogel, 2015: 9). Ello sin contar con la realización de actividades diplomáticas, como apoyo de grupos terroristas afines o programas sociales en la población para obtener su apoyo, en cuyo caso los costos se incrementan exponencialmente. Este esquema genera una gran demanda de recursos y, por consiguiente, la necesidad de canales seguros de financiamiento para la organización.

Las fuentes para procurar los recursos necesarios para mantener estas organizaciones pueden ser tantas como la imaginación permita. Sin embargo, pueden clasificarse principalmente en cuatro: donaciones, ingresos provenientes de delitos, rentas provenientes de empresas que realizan actividades lícitas y la explotación del territorio controlado (Sieber y Vogel, 2015: 10). Salvo en el último caso, los recursos obtenidos requieren ser traspasados a las arcas de la organización terrorista, lo cual puede lograrse mediante el contrabando físico de dineros u otros activos (FATF, 2015a: 29), la transferencia bancaria con ocultamiento de la identidad del emisor o receptor (FATF, 2015a: 27-28) y la transferencia de dineros a través de sistemas no regulados (Sieber y Vogel, 2015: 14).

En relación con este último método, el medio empleado hasta ese momento era el de sistemas alternativos de transferencias de valores, sean empresas especializadas no bancarias o sistemas alternativos de transferencias de valor como el *hawala*

(FATF, 2008: 24).[23] Sin embargo, con la irrupción de las monedas virtuales, es posible financiar una organización terrorista burlando todos los controles convencionales. Basta descargar un cliente Bitcoin, adquirir monedas virtuales por cualquier medio —sea mediante venta de bienes o servicios, en una casa de cambio o derechamente en el mercado negro— y transferirlas a la dirección de destino, sin que exista control alguno de la operación. El carácter irrestrictamente internacional de los sistemas de monedas virtuales facilita a los terroristas el acceso a fuentes de financiamiento lejanas y de otro modo difícilmente alcanzables.

Mención especial requiere el financiamiento de organizaciones terroristas mediante donaciones. En el último tiempo, este mecanismo ha ganado relevancia como fuente de financiamiento de operaciones terroristas, dadas las capacidades comunicacionales actuales para solicitar y coordinar donaciones de distintos actores alrededor del globo.[24] Más allá de basarse en donaciones esporádicas provenientes de individuos acaudalados,[25] hoy en día es posible sumar numerosos aportes pequeños provenientes de un gran número de individuos, mediante mecanismos de financiamiento colectivo a través de internet (*crowdfunding*). Las características pseudoanónimas del Bitcoin permiten a un mayor número de personas situadas en países diferentes efectuar sus aportes en forma indetectable y segura, los cuales pueden ser reunidos y luego transferidos directamente a la organización.

Lavado de activos, artículo 27 de la Ley 19.913

El riesgo criminógeno de las monedas virtuales se presenta en su mayor intensidad en materia de lavado de activos. Éste se define como un «proceso cuyo objeto es disimular el verdadero origen de aquellas rentas provenientes de actividades ilícitas» (Toso Milos, 2008: 406), y se encuentra tipificado en el artículo 27 de la Ley 19.913, que «Crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos». Para dimensionar la interacción entre las monedas virtuales y este delito en particular, es necesario entender las etapas a través de las cuales se lleva a cabo.

23. El *hawala* es un sistema informal de transferencias de fondos originado en el mundo árabe. Su *modus operandi* no es en base a envíos físicos o electrónicos de dinero, sino que por una red de corredores o *hawaladars* que operan como agentes (avales) de los clientes.

24. Consejo de Seguridad de Naciones Unidas, «El Estado Islámico del Iraq y el Levante y el Frente Al-Nusra para los Pueblos del Levante: Informe y recomendaciones presentados de conformidad con la resolución 2170 (2014)», informe, 14 de noviembre de 2014, p. 25, disponible en https://undocs.org/es/S/2014/815.

25. Por ejemplo, un reporte de la FATF menciona una donación efectuada en 2014 por un sujeto situado en la región del Golfo Pérsico en beneficio del Estado Islámico de Irak y el Levante, ascendiente a más de U$ 2 millones (FATF, 2015-2: 18).

Según la mayoría de la doctrina nacional e internacional y siguiendo el modelo propuesto por la FATF, el proceso de lavado de activos se compone de tres etapas: colocación (*placement*), la cual está encaminada a introducir los activos criminalmente obtenidos en el comercio legal mediante cualquier tipo de negocio; estratificación (*layering*), que tiene por fin ocultar el origen de los activos y borrar las huellas contables del mismo a través de un gran número de transacciones lo más complejas posible; y finalmente integración (*integration*), que implica conferir una apariencia de legalidad a los activos al integrarlos al sistema bancario como producto de una actividad económica lícita (Toso Milos, 2008: 407).

En este proceso, las características de las monedas virtuales son útiles para lograr el efecto buscado mediante el lavado de activos (Arias Acuña y Sánchez Pullas, 2016: 203), especialmente en la etapa de estratificación. En efecto, los activos ilegalmente obtenidos pueden cambiarse a monedas virtuales en casas de cambio,[26] transferirlas luego a una red de cuentas ubicadas en el extranjero mediante la red Tor usando al mismo tiempo servicios de mezclado, para finalmente cambiarlas a moneda de curso legal en otra casa de cambio o bien adquirir con ellas bienes y servicios a través de internet. En este proceso, el anonimato en las transacciones y la posibilidad de efectuarlas de manera transfronteriza son aspectos propicios para disimular el rastro documentado, la fuente y la propiedad de los recursos (Wright y De Filippi, 2015: 22). Estas características generan mayores dificultades para las labores de investigación y, con ello, mejores posibilidades de impunidad para los actores.

A lo anterior se suma el hecho de que todas estas transferencias y movimientos se efectúan al margen de los sistemas financieros establecidos. No existe un ente central que las administre, al estar distribuidas en un número indeterminado de usuarios. Ello redunda en la inaplicabilidad de las actuales medidas preventivas contra las operaciones de lavado de activos establecidos en los artículos 3 a 7 de la Ley 19.913, así como los deberes de organización impuestos por la Unidad de Análisis Financiero, la Superintendencia de Bancos e Instituciones Financieras y la Superintendencia de Valores y Seguros. Los diversos deberes de organización y de colaboración establecidos en la Ley[27] y normativa complementaria,[28] que tienen por objeto impedir el

26. También el producto de un delito puede llegar a manos de los delincuentes en moneda virtual sin necesidad de una casa de cambio. Ello puede ocurrir, por ejemplo, en caso de un asesinato concertado en la Darknet y pagado directamente en Bitcoin.

27. Por ejemplo, el deber de informar de operaciones sospechosas (artículo 3, inciso primero de la Ley 19.913), designar oficial de *compliance* (artículo 3, inciso cuarto), mantener registro (artículo 5) y guardar secreto (artículo 6) (Bedecarratz Scholz, 2018: 215-216).

28. Por ejemplo, el deber de instituir un proceso de aceptación de clientes que incluya recabar sus antecedentes (en caso de personas jurídicas razón social, personas que la integran, domicilio, giro, datos de contacto, etcétera), así como establecer un sistema de seguimiento o monitoreo permanente de sus operaciones, como también el deber de establecer una política de selección y capacitación permanente

aprovechamiento del sistema financiero y de otros sectores de la actividad comercial para la comisión del delito de lavado de activos, no son aplicables en su forma actual, dada la falta de sujetos obligados capaces de cumplirlos a cabalidad.

Hacia una estrategia de respuesta

Como ya se ha demostrado, la irrupción de la tecnología de las monedas virtuales ha elevado el riesgo de comisión de delitos informáticos, financiamiento del terrorismo y, especialmente, de lavado de dinero. Frente a este claro diagnóstico, existe controversia respecto al tratamiento con que los ordenamientos jurídicos deben responder frente al uso de monedas virtuales (Werbach, 2017: 34). A continuación, se analizarán desde un punto de vista dogmático las distintas alternativas existentes para prevenir su uso en actividades criminales.

Tipificación del uso de monedas virtuales como delito

Una primera posibilidad es la respuesta punible, esto es, prohibir el uso de monedas virtuales y amenazar con una pena en caso de infracción de la prohibición. Esta nueva figura penal sería un delito de riesgo abstracto, basado en consideraciones preventivas generales que apuntarían a reducir el riesgo de comisión de delitos de lavado de dinero, financiamiento del terrorismo e informáticos mediante la remoción de una herramienta especialmente apta para su comisión. Sin embargo, la alternativa de la penalización del uso de monedas virtuales debe enfrentarse a un categórico rechazo por parte de los penalistas, en virtud de los siguientes argumentos.

En primer lugar, las criptomonedas no generan *per se* un daño en la sociedad ni tampoco una puesta en peligro concreto de bienes jurídicos esenciales para la convivencia humana. Si bien pueden ser usadas como instrumentos de ciertos delitos descritos en el ordenamiento nacional, las conductas de creación, posesión, uso y transferencia de monedas virtuales no lesionan ni tampoco amenazan por sí mismas a ningún bien jurídico protegido, pues poseen un carácter neutro en términos de peligrosidad. Por lo tanto, este tipo de conductas no acarrean por sí solas un desvalor que se haga acreedor de una respuesta penal.[29] En realidad, el desvalor es generado por las conductas principales —en los ejemplos analizados el lavado de dinero, el financiamiento de terrorismo y los delitos informáticos— en las que se emplean estos instrumentos, cuando asumen más bien el carácter de una herramienta o medio para lograr el agotamiento e impunidad del delito. Salvo el caso de los delitos informáticos, en que se detectan serias fa-

---

de personal, con el objeto de contar con una colaboración efectiva por parte de todos los miembros de la organización en las tareas de prevención de blanqueo (Circular 49 de la Unidad de Análisis Financiero, 3 de diciembre de 2012, pp. 4 y ss.) (Bedecarratz Scholz, 2018: 216-217).

29. Sobre la idea del desvalor como fundamento de la pena, véase Cury Urzúa (2011: 49).

lencias en cuanto al número y amplitud de las conductas sancionadas, el ordenamiento punitivo nacional se encuentra suficientemente provisto de figuras penales para perseguir los hechos delictivos principales en los cuales se emplean monedas virtuales.

En segundo lugar y enlazando con lo anterior, el derecho penal opera solamente cuando las demás sanciones que establece el ordenamiento jurídico —sean de corte civil o administrativo— son juzgadas como insuficientes o ineficaces para preservar la paz social. En palabras de Garrido Montt (2003: 15, 40), la reacción penal será el último recurso —extremo y supremo— al que puede echar mano el ordenamiento jurídico para lograr el respeto de sus mandatos y prohibiciones. Este principio es el de *ultima ratio* o de subsidiariedad del derecho penal, pues interviene solo cuando las demás *ratios* han sido ineficaces (Rengier, 2016: 9; Wessels y Beulke, 2010: 3). Dado que el derecho penal contempla consecuencias altamente enérgicas, éstas deben ser correlativamente aplicadas en forma restrictiva por el legislador. Ello se entiende únicamente en caso de que se vulneren bienes jurídicos esenciales y reconocidos como fundamentales por todo el grupo social (Streng, 2012: 5). En este sentido, la aplicación de una sanción penal al comercio con criptomonedas no satisface las exigencias del principio y lo vulnera en su esencia.

En tercer lugar, a la alternativa de la penalización se oponen razones del efecto útil de la norma penal. En principio, la prohibición de su uso carecería de exigibilidad, habida cuenta de la dificultad técnica de imponer efectivamente la prohibición y la multitud de formas que ofrece la tecnología para evadirla. Así, una norma prohibitiva penal no solo sería inútil, sino que también afectaría la credibilidad del derecho penal para imponer sanciones, lo cual dañaría al sistema en su conjunto.

Finalmente, la alta relevancia que pueden llegar a cobrar las monedas virtuales en la vida social harían poco recomendable, en el estado actual, declarar normativamente la ilicitud de su posesión, uso o transferencia, ni menos que lleguen a ser consideradas conductas merecedoras de pena. En este sentido, la tecnología *blockchain* —una de cuyas aplicaciones son las criptomonedas— representa un avance en materia de seguridad y rapidez de transferencias, publicidad registral y contabilidad. Es un contrasentido penalizar las criptomonedas para prevenir su mal uso, pues con ello se restringiría el desarrollo de esta nueva tecnología en nuestro país e impediría su positivo impacto social.

En suma, se desaconseja la introducción de tipos penales nuevos que sancionen penalmente las operaciones con criptomonedas, en virtud del nulo desvalor de su uso, del principio de *ultima ratio*, de la eficacia de la norma penal y de la relevancia social que representa la tecnología en que se basan. La necesaria reforma del catálogo de delitos informáticos contemplados en la Ley 19.223 no debe extenderse a tipificar el comercio de criptomonedas como una conducta punible, pues sería una reacción desproporcionada al limitado uso que se le está dando y su todavía baja incidencia en comportamientos delictivos.

Autorregulación

Una propuesta diametralmente opuesta a la anterior sería que el Estado no intervenga en el funcionamiento de las monedas virtuales, sino que deje a estos sistemas en relativa libertad para que se regulen a sí mismos. Se ha postulado que un marco regulatorio externo para las monedas virtuales no sería necesario, pues la relativa baja incidencia de delitos cometidos con criptomonedas en el contexto general —comparados, por ejemplo, con delitos cometidos con armas de fuego—, haría innecesaria una regulación legal al efecto (Böhme y otros, 2017: 7). En este sentido, sistemas de rápida evolución e innovación como las criptomonedas presentarían condiciones más propicias para la autorregulación, frente a una estrategia impuesta por el Estado. A través de la creación de sistemas de organizaciones descentralizadas cada vez más complejas, la tecnología puede ser usada para establecer reglas y estructuras para este tipo de sistemas, que se harían cumplir automáticamente a través de códigos autoejecutables (Wright y De Filippi, 2017: 50).

Sin embargo, la inactividad de los reguladores estatales puede conducir a efectos indeseados al interior de los ordenamientos jurídicos. Por una parte, el mercado puede reaccionar desfavorablemente ante sectores desafectos al marco regulatorio, ignorando o derechamente obstaculizando el funcionamiento de esta industria.[30] De este modo, la falta de seguridad jurídica en la materia generaría condiciones desfavorables para las monedas virtuales e impediría su futuro desarrollo en el país.

En consonancia con lo anterior, la falta de regulación genera el riesgo de la creación de zonas francas para la actividad delictiva, ejemplo paradigmático de lo cual fue el caso Silk Road, en el que hubo un aprovechamiento de la desregulación para fomentar el financiamiento de delitos de la más variada especie. Estos fenómenos tienen un efecto criminógeno que desplaza el uso legítimo que puede dársele a estos instrumentos. Más aún, la falta de reglamentación sobre estos sistemas ha ocasionado en el pasado perjuicios para sus usuarios legítimos, pues los deja vulnerables frente a defraudaciones, actos de piratería informática u otras conductas delictivas (Trautman y Harrell, 2017: 1.093 y ss.).

Frente a estas dificultades, el riesgo que presentan las criptomonedas debe limitarse más bien a través de una estrategia regulatoria, para lo cual existen las siguientes alternativas.

30. En marzo de 2018, numerosos bancos chilenos informaron que dejarán de operar con empresas que realicen negocios con criptomonedas —incluidas Bitcoin, Ethereum, Litecoin y otras—, lo que dejó a la industria con reducidas posibilidades de operar en el país. Patricia Marchetti Michels, «Golpe a las plataformas de criptomonedas en Chile: Banca privada les cierra cuentas y firmas acusan discriminación», *Emol.com*, 26 de marzo de 2018, disponible en http://bit.ly/2HQIM24.

Integración de monedas virtuales en sistemas de prevención de lavado de activos

Un tercer curso de acción destinado a limitar el potencial criminógeno de las monedas virtuales es supeditar su comercio a las obligaciones de prevención de lavado de activos actualmente vigentes. Es posible extender los deberes de identificación, supervisión y reporte al sistema de las monedas virtuales para crear una nueva categoría de sujetos obligados. El objeto de ello es hacer aplicable por extensión el esquema diseñado en los artículos 3 a 7 de la Ley 19.913 y demás normativa complementaria a las monedas virtuales.

Esta solución es la más simple y tradicional, pues sencillamente extiende a esta realidad particular el modelo de *compliance* diseñado para responder a esta clase de riesgos delictivos (Bedecarratz Scholz, 2016: 164 y ss.). Como ya se ha adelantado, la Comisión Europea ha propuesto concretamente:

> Someter las operaciones anónimas de cambio de divisas al control de las autoridades competentes mediante la ampliación del ámbito de aplicación de la directiva contra el blanqueo de capitales para incluir a las plataformas de cambio de monedas virtuales, y someterlas a supervisión con arreglo a la legislación contra el blanqueo de capitales y la financiación del terrorismo a nivel nacional.[31]

En Chile, las casas o plataformas de cambio de criptomonedas en dinero fiduciario están inscritas en el giro de «casas de cambio» u «otras entidades facultadas para recibir moneda extranjera». Ambos tipos de entidades son sujetos obligados según el artículo 3 inciso primero de la Ley 19.913, por lo que están afectas a las obligaciones que establece la misma ley y la normativa emitida por la Unidad de Análisis Financiero, la Superintendencia de Bancos e Instituciones Financieras y la Superintendencia de Valores y Seguros.[32]

Sin embargo, la integración así concebida sería por sí sola insuficiente, pues solamente permitiría fiscalizar el cambio de monedas virtuales por dinero fiduciario o viceversa, es decir, la compra y venta que el usuario final efectúa de las mismas, pero no el comercio de monedas virtuales efectuados a través de internet (Cifuentes Hurtado, 2017: 6). La transferencia en línea de monedas virtuales no es susceptible de ser controlada mediante el esquema convencional, pues se realiza, como ya se observó, directamente entre los usuarios (*peer to peer*), sin que exista una institución intermedia que las ejecute o autorice.

En cuanto a los restantes actores del sistema, tampoco les son aplicables los debe-

31. Comisión Europea, «Comunicación de la Comisión», p. 6.

32. Los prestadores de servicios de pago en monedas virtuales quedan igualmente afectos a estos deberes, dado que entran en la categoría de «otras entidades que estén facultadas para recibir moneda extranjera».

res de prevención. Los administradores de monederos son meros programadores que ponen a disposición de los usuarios la infraestructura informática para comerciar con criptomonedas, sin ningún control sobre las transferencias. Los individuos que validan las transferencias (o mineros) tampoco pueden revisar los antecedentes de las transferencias, pues tienen por función únicamente la certificación de la validez técnica y no la revisión de la conformidad normativa de las operaciones.

Por todo lo anterior, falta un sujeto pasivo de las obligaciones de *compliance* establecidas en la Ley 19.913 y demás normativa complementaria que pueda actuar como sujeto activo de las acciones correlativas de identificación, supervisión y reporte. Las características del comercio Bitcoin hacen imposible una regulación efectiva por esta vía (Böhme y otros, 2017: 1).

En consecuencia, la solución es insuficiente para regular el mal uso que los usuarios pueden dar a las criptomonedas, por lo que es necesario un nuevo enfoque para mantener el comercio con estos instrumentos dentro del marco de la legalidad.

Creación de un nuevo enfoque regulatorio

Decantados en favor de un modelo regulatorio y al ser insuficientes por sí solos los sistemas convencionales para la prevención de delitos, debemos construir un modelo nuevo para el control de las monedas virtuales. Una respuesta acorde debe considerar en su diseño el particular funcionamiento y características de estos instrumentos.

Previo a revisar las alternativas existentes, cabe aclarar que alterar los protocolos de funcionamiento de las monedas virtuales con el fin de acomodar controles adicionales a nivel sistémico requeriría el consentimiento de al menos el 50% del poder de procesamiento de los usuarios de la red (Nakamoto, 2008: 1). Por lo tanto, no es factible obligar al sistema de moneda virtual a detener una transferencia identificada como una operación sospechosa, como sí lo podría hacer un banco que se enfrenta a la misma situación con uno de sus clientes.

A lo anterior se suma que no es factible obligar directamente a los usuarios finales mediante normas regulatorias, dado su número, dispersión geográfica y la falta de tecnología adecuada para su control. El pseudoanonimato y descentralización a los que ya se ha hecho referencia implican que sea complejo hacer cumplir las obligaciones regulatorias de un modelo semejante (Böhme, 2017: 11). Las propuestas regulatorias solo pueden considerar a ciertos actores especiales, que en base a sus roles en el sistema de criptomonedas tienen capacidad de implementar la norma regulatoria. En consideración con lo anterior, este trabajo expone dos enfoques regulatorios, diferenciables según los sujetos obligados a implementarlos.

El modelo redlist

Un primer enfoque se basa en que los mineros se transformen en sujetos obligados e implementen controles de legalidad de las transacciones, lo que modifica la función de minería o procesamiento de las transacciones. Este control operaría no a través de la alteración del sistema de criptomonedas, sino que mediante el cambio de los programas que son empleados por los usuarios. En concreto, la forma como ello puede operar es a través de un sistema de «lista roja» o *redlist* (Pouwelse, 2014: 1).

La propuesta implica identificar aquellas direcciones o cuentas involucradas en actividades delictivas, las cuales luego serían incorporadas por el ente regulador en una lista única centralizada. Esta *redlist* sería incorporada en el software usado por los mineros, el cual se abstendría de procesar y certificar transacciones vinculadas a direcciones o cuentas registradas en ella (Pouwelse, 2014: 5). El no procesamiento de las transacciones por parte de los mineros transformaría a las direcciones o cuentas comprometidas en actividades delictivas en prácticamente inútiles, pues no podrían enajenar las monedas virtuales destinadas a ellas. Ello desincentivaría el uso de criptomonedas en actividades criminales, pues limitaría su comerciabilidad y conjuntamente su aprovechamiento por los delincuentes.

Si bien parte de una premisa novedosa, este modelo no promete ser efectivo, pues bastaría con usar otro software de minería que no tenga instalado el control para eludir al sistema. Por otra parte, la norma regulatoria carecería de eficacia, pues no es posible controlar que el usuario esté empleando el software legal, sin invadir al mismo tiempo su sistema informático. Ello constituiría una intolerable vulneración a la privacidad de los usuarios legales.

El modelo blacklist

La segunda propuesta considera como destinatarios de la regulación a aquellos actores que conectan los sistemas de monedas virtuales con los sistemas monetarios regulados (FATF, 2015b: 6-7). Actualmente, éstos son las casas de cambio y los proveedores de servicios de pago. La estrategia emplea el sistema *blockchain* en contra de los mismos delincuentes que buscan aprovecharse de él, al implementar un sistema de «lista negra» o *blacklist* (Böhme y otros, 2017: 1).

Recordando lo ya expuesto, la cadena de bloques es una especie de registro de contabilidad pública compartido que incluye todas las transacciones confirmadas. Por tanto, en caso de que llegue a conocimiento de los entes reguladores (nacionales o internacionales) de que una transacción de criptomonedas es producto de un ilícito, entonces es posible identificar con precisión el bloque del *blockchain* que registra la transacción y, por lo tanto, también a las criptomonedas específicas que fueron usadas en dicho acto. En tal caso, las monedas virtuales en cuestión pueden ser in-

corporadas en un registro público y abierto (la *blacklist*), lo que obliga a las casas de cambio y a prestadores de servicios de pago en Chile a no aceptar monedas que han sido incluidas en él. A estos sujetos obligados se les puede amenazar con una sanción administrativa correspondiente a una multa para el caso de infracción (Böhme y otros, 2017: 10).

Este enfoque combina el sistema internacional de listas de personas afectas a un embargo o sospechosas de delitos terroristas[33] con la técnica de los billetes marcados producto del robo de un cajero automático. Dado que se limita la comerciabilidad de monedas virtuales cuestionadas, lo que impide su cambio a dinero fiduciario en el ordenamiento jurídico chileno, se obliga indirectamente a los usuarios a no aceptar monedas virtuales involucradas en actividades delictivas. La individualización de todas aquellas monedas sospechosas de haber sido utilizadas en actividades delictivas en un listado público, accesible para las casas de cambio, proveedores de servicios de pago y demás interventores en el sistema, amplía el efecto de la regulación a los usuarios finales, lo cual incentiva un interés directo en no aceptar las monedas cuestionadas.

Esta medida tiene el potencial de impedir que el producto de delitos sea aprovechado mediante la venta en Chile de criptomonedas. Además, tiene el potencial de restringir el uso de criptomonedas en cualquier tipo de delito, pues desincentiva su uso en actividades criminales a través de un efecto en cadena, cuyo primer eslabón es el delincuente y el último la casa de cambio encargada de ejecutar la regulación.

En relación con lo anterior, se puede presentar el problema de que una misma transacción consista de criptomonedas incriminadas e incluidas en la *blacklist*, junto a otras sin tal carácter. En este caso, surge la dificultad de cómo debe proceder el sujeto obligado frente a este acto. En principio, no es posible rechazar la totalidad de la transferencia, pues se estaría injustamente impidiendo la comerciabilidad de monedas que no han sido cuestionadas, lo que afecta indebidamente el derecho de propiedad del tradente sobre ellas. Una posible solución a este inconveniente sería que el sujeto obligado —una casa de cambio, por ejemplo— aplique una rebaja o *haircut* a la transferencia y cambie solo aquellas monedas no incriminadas (Böhme y otros, 2017: 10). De este modo, se impide la comerciabilidad de las monedas incriminadas sin embarazar la libre circulación de las demás.

Finalmente, la implementación de este enfoque regulatorio requiere la existencia de un organismo público, encargado de confeccionar y publicar la *blacklist* y dotado de los medios y facultades necesarios para cumplir con esta labor. En particular, esta-

33. Por ejemplo, la lista de sancionados creada y mantenida de conformidad con las Resoluciones 1.267 (1999), 1.989 (2011) y 2.253 (2015) del Consejo de Seguridad de las Naciones Unidas, relativas al denominado Estado Islámico de Irak y el Levante (Daesh), Al-Qaeda y las personas, grupos, empresas y entidades asociadas con dichas organizaciones.

rá encargado de incorporar las monedas virtuales incriminadas en el registro público, de difundirlo a los actores relevantes, fiscalizar su cumplimiento e imponer sanciones administrativas para el caso de su contravención. Como organismo administrador puede pensarse en la Unidad de Asuntos Financieros, la cual ya tiene como función la prevención de los delitos de lavado de activos y de financiamiento de terrorismo en el sector financiero. Las facultades coordinadoras, fiscalizadoras y sancionadoras establecidas en el artículo 2 de la Ley 19.913 pueden extenderse en materia de prevención de delitos con monedas virtuales. De este modo, se evitaría la creación de un servicio público especializado, con el costo que ello implica. Finalmente, se aprovecharían las competencias del organismo en la materia, lo que generará sinergias desde una perspectiva funcional al interior del mismo.

Conclusiones

Las monedas virtuales son una nueva herramienta tecnológica que, en breve tiempo, ha alcanzado una fuerte presencia en el debate público. Junto con sus potenciales usos, como la protección de privacidad, facilidad de operaciones internacionales y reducción de costos de transferencias, constituyen también una fuente de riesgos que pueden ocasionar una más difícil persecución de hechos punibles. En concordancia con las recomendaciones planteadas por diversos organismos internacionales, como el Banco Central Europeo, la Autoridad Bancaria Europea y el Grupo de Acción Financiera contra el Blanqueo de Capitales, así como nuestra propia Unidad de Asuntos Financieros, se hace necesario observar atentamente la evolución en el funcionamiento y uso de las monedas virtuales, para así diseñar medidas eficaces que neutralicen el potencial criminógeno que ofrecen.

Frente a esta realidad, actualmente no es aconsejable seguir una solución exclusivamente penal ni tampoco de absoluta autorregulación, sino que es preferible optar por una respuesta regulatoria. En este sentido, la aplicación del modelo regulatorio tradicional en contra del lavado de activos, terrorismo y otros hechos punibles, que extiende lisa y llanamente la lista de sujetos obligados y mantiene los actuales deberes de identificación, supervisión y reporte, resultaría totalmente insuficiente frente a la realidad descrita. La dispersión del comercio de criptomonedas entre un número indeterminado de sujetos, repartidos por añadidura en múltiples jurisdicciones a lo largo de todo el mundo, hace que sea imposible establecer un sistema efectivo.

Por lo tanto, es necesario que el Legislador asuma esta realidad mediante un modelo regulatorio especializado, que responda a la particular estructura y funcionamiento de las monedas virtuales. En este sentido, se postula crear un registro de transacciones involucradas en actividades ilícitas e imponer una prohibición para ciertos actores de aceptar las monedas virtuales que hayan sido objeto de este tipo de transferencias. De este modo, se aprovecha la arquitectura de los sistemas de mone-

das virtuales, específicamente el *blockchain*, para mantener su uso en el marco de la legalidad. Así, esta estrategia tendría el potencial de limitar los daños sociales generados por el mal uso de las monedas virtuales e integrarlas al tráfico jurídico mediante una regulación adecuada y efectiva.

Referencias

Acuña Sáez, Héctor (2017). «Estudio sobre Bitcoin y tecnología *blockchain*». ESE Business School, Universidad de Los Andes, Chile. Disponible en http://bit.ly/2y8n5uG

Arias Acuña, Gonzalo y Andrés Sánchez Pullas (2016). «The digital currency challenge for the regulatory regime». *Revista Chilena de Derecho y Tecnología*, 5 (2): 173-209. DOI: 10.5354/0719-2584.2016.43541.

Bedecarratz Scholz, Francisco Javier (2016). *Rechtsvergleichende Studien zur Strafbarkeit juristischer Personen. Eine Untersuchung ihrer Strafzurechnungsmerkmale in den Rechtsordnungen von Chile, Deutschland, England, Frankreich, Spanien und den Vereinigten Staaten*. Baden-Baden: Nomos-Verlagsgesellschaft.

—. (2018). «La indeterminación del *criminal compliance* y el principio de legalidad». *Política Criminal*, 13 (25): 208-232. DOI: 10.4067/S0718-33992018000100208.

Böhme, Rainer, Johanna Grzywotz, Paulina Pesch, Christian Rückert y Christoph Safferling (2017). «Prävention von Straftaten mit Bitcoins und Alt-Coins. Handlungsempfehlung zur Regulierung virtueller Kryptowährungen». Bitcrime. Disponible en http://bit.ly/2MonHVd.

Cifuentes Hurtado, María Cecilia (2017). «Bitcoin y criptomonedas: Concepto, regulación, uso como medio de pago y potenciales efectos en los mercados financieros locales». ESE Business School, Universidad de Los Andes, Chile. Disponible en http://bit.ly/2M2yuOG.

Cury Urzúa, Enrique (2011). *Derecho penal: Parte general*. 10.ª ed. Santiago: Ediciones UC.

FATF, Financial Action Task Force (2008). «Terrorist financing typologies report». Financial Action Task Force. Disponible en http://bit.ly/2M3bjnI.

—. (2014). «FATF report, virtual currencies, key definitions and potential AML/CFT risks». Financial Action Task Force. Disponible en http://bit.ly/2Mopj1d.

—. (2015a).«Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL)». Financial Action Task Force. Disponible en http://bit.ly/2LYATdo.

—. (2015b). «Guidance for a risk-based approach to virtual currencies». Financial Action Task Force. Disponible en http://bit.ly/2LZ8nZe.

Garrido Montt, Mario (2003). *Derecho penal: Parte general*. Tomo 1. Santiago: Jurídica de Chile.

Hamari, Juho, Mimmi Sjöklint y Antti Ukkonen (2015). «The sharing economy: Why people participate in collaborative consumption». *Journal of the Association for Information Science and Technology,* 67 (9): 2.047-2.059. DOI: 10.1002/asi.23552.

Harris, Laurence (1993). *Teoría monetaria*. Ciudad de México: Fondo de Cultura Económica.

Huerta Miranda, Marcelo y Claudio Líbano Manzur (1996). *Delitos informáticos*. Santiago: Jurídica Conosur.

Magliona Markovicth, Claudio Paul y Macarena López Medel (1999). *Delincuencia y fraude informático*. Santiago: Jurídica de Chile.

Nakamoto, Satoshi (2008). «Bitcoin: Un sistema de efectivo electrónico usuario-a-usuario». Disponible en https://bitcoin.org/es/bitcoin-documento.

Politoff Lifschitz, Sergio, Jean Pierre Matus Acuña, y María Cecilia Ramírez Guzmán (2016). *Lecciones de derecho penal chileno: Parte general*. 2.ª ed. Santiago: Jurídica de Chile.

Pouwelse, Johan (2014). «Operational distributed regulation for Bitcoin». Disponible en https://arxiv.org/abs/1406.5440.

Rengier, Rudolf (2016). *Strafrecht Besonderer Teil I*. Múnich: Verlag CH Beck.

Rogojanu, Angela y Liana Badea (2014). «The issue of competing currencies». *Theoretical and Applied Economics,* 21 (1): 103-114. Disponible en http://bit.ly/2Mot1rF.

Sieber, Ulrich y Benjamin Vogel (2015). *Terrorismusfinanzierung. Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht*. Berlín: Duncker & Humblot.

Streng, Franz (2012). *Strafrechtliche Sanktionen. Die Strafzumessung und ihre Grundlagen*. 3.ª ed. Constanza: Kohlhammer-Verlag.

Toso Milos, Ángela (2008). «Blanqueo de capitales su prevención en el ordenamiento jurídico chileno». *Revista Chilena de Derecho,* 35 (3): 405-437. DOI: 10.4067/S0718-34372008000300002.

Trautman, Lawrence y Alvin Harrell (2017). «Bitcoin versus regulated payment systems: What gives?». *Cardozo Law Review,* 38 (3): 1.041-1.097. DOI: 10.2139/ssrn.2730983.

Werbach, Kevin (2017). «Trust, but verify: Why the blockchain needs the law». *Berkeley Technology Law Journal,* (inédito). DOI: 10.2139/ssrn.2844409.

Wessels, Johannes y Werner Beulke (2010). *Strafrecht Allgemeiner Teil. Die Straftat und ihr Aufbau*. 40.ª ed. Heidelberg: CF Müller-Verlag.

Wright, Aaron y Primavera de Filippi (2015). «Decentralized blockchain technology and the rise of *Lex Cryptographia*». DOI: 10.2139/ssrn.2580664.

Sobre el autor

Francisco Bedecarratz Scholz es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad Autónoma de Chile. Magíster y Doctor en Leyes por la Universidad de Marburgo, Alemania. Profesor de la Facultad de Derecho de la Universidad Autónoma de Chile. Su correo electrónico es francisco.bedecarratz@uautonoma.cl.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).