Artículos

Revista Pensamiento Penal
Sección Derecho penal
Vol. 2, núm. 4 – 2025, págs. 85–124
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/p7xqrm42

Análisis del impacto de las criptomonedas en el lavado de activos: desafíos y perspectivas en el contexto actual

Sebastián Jáuregui[1]

Resumen

Desde la aparición de bitcoin en 2009, las criptomonedas y la tecnología blockchain han revolucionado el panorama financiero y tecnológico. Si bien ofrecen beneficios como transacciones rápidas y menores comisiones, su naturaleza descentralizada y el anonimato que pueden proporcionar plantean serios desafíos en la lucha contra el lavado de activos. Las criptomonedas, al carecer de una autoridad central y permitir movimientos transfronterizos con gran facilidad, se han convertido en una herramienta atractiva para delincuentes que buscan ocultar el origen ilícito de fondos. Las etapas tradicionales del lavado de activos (colocación, ocultación y reintroducción) se adaptan a su uso, facilitando la fase de ocultación con mayor velocidad y anonimato, lo que complica enormemente las investigaciones. Organismos internacionales como el GAFI y entidades locales como la UIF han advertido sobre estos riesgos, señalando la dificultad de rastrear e incautar bienes en un sistema descentralizado. Este escenario subraya la urgente necesidad de analizar el impacto de las criptomonedas en el lavado de activos, identificar las técnicas empleadas y desarrollar estrategias regulatorias y de combate efectivas. La investigación se propone abordar estos desafíos, buscando comprender cómo se utilizan las criptomonedas para fines delictivos y proponer recomendaciones para mitigar este riesgo creciente.

Sumario

Palabras clave

criptomonedas – lavado de activos – tecnología blockchain – criptoactivos – compliance

[1] Abogado (Universidad Católica de La Plata). Especialista en Cibercrimen (Universidad Siglo 21). Instructor judicial en la U.F.I. No. 2 Departamento Judicial de Mercedes, provincia de Buenos Aires. Correo electrónico: sjaureguiabogado@gmail.com

1. Análisis del tipo penal en la ley 22.421 y relación con el código penal

Las criptomonedas, como bitcoin, ethereum y otras altcoins, son monedas digitales que utilizan criptografía para asegurar las transacciones y controlar la creación de nuevas unidades. Estas monedas operan en un entorno virtual y no están respaldadas por ningún gobierno o entidad central, lo que las hace atractivas para aquellos que buscan el anonimato en sus transacciones financieras.

En búsqueda de una definición conceptual de criptomoneda, encontramos la propuesta por el *grupo de acción financiera internacional* (en adelante, «GAFI»), que las describe como «la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción» (GAFI, 2015: 32).

Por su parte, Lansky (2018), las define como un medio digital de intercambio que utiliza la criptografía para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos.

Precisamente, una de las características inherentes a las criptomonedas es la capacidad de realizar transacciones de forma pseudónima o incluso anónima. Aunque las transacciones se registran en una cadena de bloques pública, las identidades de los participantes no están directamente vinculadas a las direcciones de criptomonedas utilizadas. Esto dificulta el rastreo de las transacciones y la identificación de los involucrados en actividades delictivas.

En este sentido, Valdés Trapote (2022: 10) explica que:

> los criptoactivos alcanzan (…) riesgos potenciales en el lavado de activos (...) las criptomonedas normalmente se basan en complejas infraestructuras que incluyen numerosas entidades o servidores, a menudo distribuidas por varios países, tanto para transferir fondos como para ejecutar pagos. Esta segmentación de servicios hace que el cumplimiento de la normativa contra el lavado de activos, así como su supervisión y ejecución no quede del todo clara. Además, registros de clientes y de transacciones pueden quedar en diferentes entidades, a menudo en diferentes jurisdicciones, haciendo mucho más difícil a investigadores y reguladores acceder a esos registros. Este problema queda exacerbado por la rápida naturaleza descentralizada de la tecnología de los activos virtuales, los cuales pueden ser instalados en jurisdicciones que no tengan adecuados controles contra el lavado de activos.

Por otro lado, sabido es que en el proceso de lavado de activos se reconocen generalmente tres etapas: colocación, estratificación e integración. La colocación implica introducir los fondos ilegales en el sistema financiero, la estratificación consiste en realizar múltiples transacciones para ocultar el origen de los fondos, y la integración busca incorporar los fondos ya lavados en la economía legítima.

El GAFI proporciona la siguiente definición sobre el delito apuntado:

> a) La conversión o transferencia de propiedad, a sabiendas de que deriva de un delito criminal, con el propósito de esconder o disfrazar su procedencia ilegal o el ayudar a cualquier persona involucrada en la comisión del delito a evadir las consecuencias legales de su accionar; b) la ocultación o disfraz de la naturaleza real, fuente, ubicación, disposición, movimiento, derechos con respecto a, o propiedad de, bienes

> a sabiendas de que derivan de ofensa criminal; c) la adquisición, posesión o uso de bienes, con el conocimiento al momento de su recibo, que deriva de una ofensa criminal o de la participación en algún delito.

Por su parte, Gómez Iniesta (1996: 86) define el blanqueo de capitales como «aquella operación a través de la cual el dinero de origen siempre ilícito es invertido, ocultado, sustituido o transformado y restituido a los circuitos económicos-financieros legales, incorporándose a cualquier tipo de negocio como si se hubiera obtenido de forma lícita».

Las criptomonedas pueden facilitar estas etapas al permitir la transferencia rápida y anónima de fondos a través de diferentes cuentas y plataformas. En directa vinculación con lo anterior, Valdés Trapote (2022: 5) señala que:

> Tomando como base las tradicionales fases que se dan en el delito de lavado de activos (colocación, ocultación y reintroducción), se adaptan sus fases a su realización mediante criptoactivos. Una de las peculiaridades de la etapa de ocultación es que la misma se ejecuta con mayor facilidad, velocidad y anonimato, lo que dificulta mucho la investigación y, por tanto, seguir el rastro del dinero.

También Donna (2021: 207) comulga con esta idea, al expresar:

> los activos ilegalmente obtenidos pueden cambiarse a monedas virtuales en casas de cambio, transferirlas luego a una red de cuentas ubicadas en el extranjero mediante la red Thor 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. En efecto, los activos ilegalmente obtenidos pueden cambiarse a monedas virtuales en casas de cambio, transferirlas luego a una red de cuentas ubicadas en el extranjero mediante la red Thor 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.

Lo expuesto da cuenta que el uso de criptomonedas en el lavado de activos plantea riesgos significativos. La naturaleza global de las criptomonedas y su capacidad para realizar transacciones transfronterizas sin intermediarios dificultan la supervisión y el seguimiento por parte de las autoridades. Además, los delincuentes pueden aprovechar las brechas en la regulación y el cumplimiento para utilizar intercambios de criptomonedas sin controles adecuados, lo que facilita el lavado de activos.

Aunque la relación entre criptomonedas y lavado de activos es una preocupación creciente, los esfuerzos regulatorios y de cumplimiento también han aumentado. Muchos países han implementado regulaciones y requisitos de debida diligencia para los proveedores de servicios relacionados con criptomonedas, como los intercambios. Además, se han propuesto iniciativas y medidas internacionales para fortalecer la supervisión y la cooperación entre jurisdicciones.

a. Origen y desarrollo del concepto de criptomoneda, en especial bitcoin

Las raíces del concepto de criptomoneda podemos encontrarla en trabajos académicos de la década de 1980 sobre criptografía y la teoría de la computación distribuida. Autores como David Chaum, en su trabajo *blind signatures for untraceable payments* (1982), y Wei Dai, quien propuso el concepto de *b-money* en 1998, sentaron las bases teóricas para las monedas digitales descentralizadas. Chaum exploró la posibilidad de utilizar la criptografía para garantizar el anonimato en las transacciones financieras, mientras que Dai sugirió un sistema de dinero electrónico descentralizado.

Sin embargo, no fue sino hasta la creación del bitcoin -atribuida a un sujeto o grupo de personas bajo el seudónimo de Satoshi Nakamoto, en noviembre del año 2008- que se produjo un avance revolucionario en la materia. En efecto, el documento publicado por Nakamoto, titulado *bitcoin: a peer-to-peer electronic cash system*, propuso la creación de un sistema de efectivo electrónico completamente descentralizado basado en una red peer-to-peer y tecnología de blockchain.

El surgimiento de las criptomonedas puede considerarse como una respuesta indirecta a la crisis financiera de Estados Unidos que tuvo su punto álgido en 2008. Aunque el desarrollo de las criptomonedas, en particular del bitcoin, no puede atribuirse directamente a esta crisis, es importante considerar el contexto económico y social en el que surgieron.

La crisis financiera de 2008 fue desencadenada por una combinación de factores, incluyendo la burbuja inmobiliaria, la proliferación de productos financieros complejos y riesgosos, y la falta de regulación adecuada en el sector financiero. Como consecuencia, hubo una pérdida masiva de confianza en las instituciones financieras tradicionales y en el sistema monetario convencional.

En este contexto de desconfianza hacia las instituciones financieras y gobiernos, surgió un mayor interés en alternativas descentralizadas y autónomas. El documento técnico publicado por Satoshi Nakamoto en 2008, justo después del estallido de la crisis financiera, es indicativo de este clima de descontento y búsqueda de soluciones alternativas.

El bitcoin se presentó entonces como una moneda digital descentralizada que operaba fuera del control de entidades gubernamentales y bancarias. Al utilizar tecnología blockchain y criptografía, el Bitcoin ofrecía un sistema de pagos peer-to-peer que no requería intermediarios financieros tradicionales. En otras palabras, el Bitcoin vino a ofrecer una nueva forma de hacer transacciones sin la necesidad de intermediarios, con una moneda cuyo suministro estaba fijado desde el principio.

En este sentido, las criptomonedas como el bitcoin surgieron en parte como respuesta al deseo de tener un sistema monetario más transparente, resistente a la censura y no sujeto a las fluctuaciones y decisiones políticas de los gobiernos y bancos centrales. Y si bien no resolvieron directamente los problemas causados por la crisis financiera de Estados Unidos, sí proporcionaron una alternativa que cuestionaba el paradigma establecido de moneda y sistema financiero. Su crecimiento y adopción desde entonces han sido impulsados por una combinación de factores, incluyendo la innovación tecnológica, la especulación financiera y la búsqueda de una mayor autonomía y control sobre el propio dinero.

De hecho, a partir del nacimiento del bitcoin han surgido otras criptomonedas alternativas, conocidas como altcoins, cada una con sus propias características y aplicaciones. Ethereum, por ejemplo, lanzada en 2015 por Vitalik Buterin, introdujo contratos inteligentes a la funcionalidad de blockchain y fue la primera blockchain con un lenguaje de programación Turing completo incorporado.

A lo largo de los años, se ha observado cómo las criptomonedas han ganado una mayor aceptación y reconocimiento a nivel mundial. Grandes instituciones financieras, como PayPal y Square, han comenzado a permitir transacciones con criptomonedas, y países como El Salvador han adoptado el Bitcoin como moneda de curso legal.

b. Definición, características

En Argentina, en el art. 2º de la resolución 300/2014 de la unidad de información financia, las monedas virtuales se definen como

> […] la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

A continuación, en el segundo párrafo del art. citado, las diferencian específicamente del dinero electrónico, entendido como «[...] un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción».

Algunos autores también han brindado sus aportes a la tarea de definir y/o conceptualizar qué entendemos cuando hablamos de criptomoneda. En este sentido, Lansky (2018) entiende que se trata de un medio digital de intercambio que utiliza la criptografía para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos.

Sánchez (2017) considera que «una criptomoneda, criptodivisa es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido».

Continuando en la búsqueda de la definición conceptual de criptomoneda encontramos la propuesta por el GAFI (2015: 32), que la describe como

> la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Ahora bien, uno de los valores añadidos que tiene en términos político-criminales la definición del GAFI es que le reconoce a la moneda virtual las principales utilidades del dinero: depósito de valor, unidad de cuenta y medio de pago. De igual modo, resalta las características de las criptomonedas, que bien podrían resumirse de modo consensuado en las siguientes: seguridad, descentralización y anonimato.

Al respecto, Navarro Cardoso (2019) explica:

> [...] La seguridad la aporta(n) las funciones resumen que permiten ser resistentes frente a ataques que intenten vulnerar la seguridad del sistema (autenticidad), así como la tecnología blockchain (trazabilidad) que le sirve de soporte. En la medida

> en que una vez que la transacción es insertada en un bloque, este es sellado y se une al siguiente, se le dota a aquella, a la transacción, de una seguridad tal que aporta soluciones sólidas frente a los fraudes que propician otras monedas digitales clásicas, más conocidas como dinero electrónico, caso de las tarjetas de créditos, así como en relación con determinados problemas propios de las monedas virtuales.
>
> […] La descentralización es la segunda gran característica: […] las transacciones se incorporan a un bloque, y bloque a bloque se añaden en un libro contable distribuido entre múltiples equipos o nodos. A diferencia de las formas de pago centralizadas, donde se suelen anotar las operaciones en un servidor único..., en la blockchain, ese libro de contabilidad distribuido, las transacciones se incorporan, primero en uno de los nodos participantes, y luego se transmiten al resto conectados en la red. Cada una de estas transmisiones se denomina «confirmación».
>
> La última característica es el anonimato. Probablemente sea la cuestión más controvertida, pues mientras unos sostienen que el anonimato es tal, otros lo matizan, y otros, claro está, lo niegan.
>
> De entrada, suele distinguirse entre anonimato y privacidad. El anonimato va referido a las personas: se ignora el remitente y el destinatario. La privacidad tiene que ver con el objeto: se desconoce el objeto de la transacción y su valor, pero no sus actores.
>
> Por un lado, no es necesaria la cesión de datos personales para crear carteras ni realizar transacciones. Sí es necesario un identificador pseudoaleatorio asociado a una cartera […] Otra cosa es cómo realizamos la transacción, pues en función de ello el anonimato puede comenzar a desaparecer, hasta llegar a ser inexistente, del mismo modo que puede casi mantenerse […]
>
> Se puede obtener mucha información a partir de una dirección o transacción, caso del balance de bitcóin o del historial de transacciones, así como del flujo del dinero, cash-out, conectividades, zona horaria y geolocalización aproximada del dueño. En cualquier caso, resulta extremadamente difícil lograr la atribución nominal de una dirección o cartera de bitcóin, a no ser que haya habido fallos de seguridad en las operaciones realizadas.

c. Tecnología blockchain o cadena de bloques

Las criptomonedas, según Nakamoto (2008), son activos digitales que emplean técnicas criptográficas para asegurar transacciones financieras, controlar la creación de nuevas unidades y verificar la transferencia de activos. Su aparición ha marcado un hito en la historia de la tecnología financiera, al ofrecer una alternativa descentralizada y segura a las monedas fiduciarias tradicionales.

Ahora bien, para empezar a comprender el funcionamiento de las criptomonedas se hace necesario, en primer lugar, conocer el ecosistema sobre el cual descansa su arquitectura, representado en este caso por la tecnología de cadena de bloques, también conocida como blockchain.

Al respecto, Zoccaro (2020) opina que la columna vertebral de las criptomonedas es la criptografía -de ahí su denominación como cripto-, y que la tecnología que hace realidad el sistema es la cadena de bloques -o blockchain-, a la cual define como una «[...] enorme base de datos almacenada en forma virtual y donde cada usuario del sistema tiene una copia actualizada y totalmente sincronizada en su computadora».

Profundizando en el concepto, explica:

> Se (la) puede imaginar también como un gran libro electrónico de actas donde se registran operaciones o sucesos, pero en lugar de existir un escribano que certifique estas actas una a una, esta validación la efectúa el conjunto de usuarios del sistema, sin necesidad de agentes externos o intermediarios y gracias al uso de la criptografía. Y una vez plasmada en la blockchain, la información no puede ser borrada ni modificada. Además, la información contenida en estos bloques es de acceso público para todos los usuarios, salvo por ciertos datos privados: así se posibilita el control sobre las transacciones.

En similar sentido, Navarro Cardoso (2019) afirma que

> […] blockchain es un gran libro de contabilidad, una gran base de datos, donde ningún asiento se puede borrar o modificar, y que no lo gestiona una sola persona, sino muchísimas, pues cada una -con su máquina- hace un asiento, de manera que una modificación exigiría que todas esas personas se pongan de acuerdo.

Y a continuación agrega

> [...] El libro funciona concatenando bloques, el anterior con el siguiente, formando una cadena. El bloque se 'sella' incluyendo un código alfanumérico, producto del recurso a tecnología algorítmica, llamado hash. Cada bloque nuevo debe contener el hash del bloque anterior. Por lo tanto, cada bloque nuevo que se une a la cadena posee todo el historial de la transacción.

Desde la perspectiva apuntada, podemos afirmar que Blockchain es una tecnología de registro distribuido que permite a los participantes de una red compartir datos de manera segura, transparente e inmutable. En lugar de almacenar información en un único servidor centralizado, la blockchain utiliza una red de nodos interconectados para mantener una base de datos descentralizada y distribuida.

En esencia, una blockchain es una cadena de bloques de datos enlazados mediante técnicas criptográficas. Cada bloque contiene un conjunto de transacciones verificadas, y cada nuevo bloque está vinculado al bloque anterior, formando así una cadena continua de datos.

La seguridad y la integridad de la blockchain se basan en la criptografía y el consenso distribuido. Cada transacción en la blockchain es verificada y validada por los nodos de la red, y una vez que se agrega un bloque a la cadena, es prácticamente imposible modificarlo sin el consenso de la mayoría de los participantes en la red. Esto crea un registro permanente e inmutable de todas las transacciones realizadas en la red.

La blockchain se utiliza principalmente como la infraestructura subyacente de las criptomonedas, pero su aplicación se extiende a una amplia gama de campos, y su potencial radica, fundamentalmente, en su capacidad para proporcionar un registro seguro y transparente de transacciones sin la necesidad de una autoridad central.

¿Cómo funciona entonces Bitcoin?

Como dijimos más arriba, la cadena de bloques -blockchain- es la columna vertebral de Bitcoin, una suerte de libro de contabilidad público y descentralizado que registra todas las transacciones de Bitcoin.

El libro funciona concatenando bloques -nodos-, formando una cadena. Los bloques contienen información sobre cada transacción, como el comprador y el vendedor, fecha

y hora, valor total y un código de identificación único para cada operación. Las entradas están conectadas en secuencia cronológica, formando una cadena digital de bloques.

El bloque se sella con la incorporación de un código alfanumérico conocido como hash, y luego pasa a formar parte de esa cadena. Cada bloque nuevo debe contener el hash del bloque anterior. Esto crea una cadena de bloques que es resistente a la manipulación y garantiza la integridad de las transacciones.

Ahora bien, para incorporarse a la cadena de bloques, las transacciones deben verificarse. Aquí entran en juego los mineros, cuya tarea consiste, según Lara y Muñoz (2017) en ejecutar «en sus máquinas software para resolver complejos cálculos matemáticos (llamados hashes) basados en criptografía con el fin de procesar y validar las transacciones». Estos problemas matemáticos se denominan *proof of work* (prueba de trabajo) y su resolución demanda un gran poder computacional y de procesamiento, que a su vez se traduce en un elevado costo energético.

Como contraprestación, los mineros obtienen una recompensa, ya que ponen a disposición de la red sus propios recursos. Al respecto, Navarro Cardoso (2019) aclara que, en realidad,

> [...] el minero recibe dos estipendios. El primero puede ir anejo a la propia transacción que se lanza a la red por quien quiere realizarla. A fin de lograr que se interesen por ella y la gestionen (la confirmen), ofrece una comisión. Cuanto más atractiva resulte, mayores probabilidades de que un minero le preste su atención. (…) El segundo estipendio es la conocida recompensa, que la genera automáticamente el sistema cuando se consigue (aleatoriamente) cerrar un bloque.

A modo de síntesis, dice Skalany (2019)

> Sólo quien resuelva o supere la prueba de trabajo tiene la capacidad de cerrar un nuevo bloque de la cadena y los restantes nodos operan como una suerte de auditores de la legitimidad y validez de la prueba superada brindando el consenso para que el bloque sea agregado de forma legítima a la cadena. La dificultad de superar la prueba de trabajo para generar un nuevo bloque se incrementa automáticamente para aproximarse a una temporización de generar un bloque cada 10 minutos. La cantidad de bitcoins nuevos que el sistema produce irá decreciendo en el tiempo, pues el sistema fue pensado para contener un total de 21.000.000 de bitcoins […]

Por otro lado, todos los usuarios que quieran enviar o recibir Bitcoins necesitan un bitcoin wallet, que pueden ser de software -en línea- o de hardware -dispositivos físicos.

Según la explicación que proporciona Small (2015)

> Estas billeteras digitales contienen una clave pública y una clave privada (conocidas como keys); la clave pública es similar a una dirección de correo electrónico que un usuario compartirá con otros usuarios de Bitcoin para que puedan enviar bitcoins. Alternativamente, la clave privada es similar a un número pin para una tarjeta de débito, cuyo propósito es confirmar que un usuario desea gastar bitcoins en su cartera.

Ampliando esta noción, Mora (2015) dice que

> […] para obtener y transferir la titularidad de los bitcoins se utiliza un mecanismo llamado 'criptografía asimétrica de clave pública'. En este esquema, cada persona que quiere constituirse como titular de bitcoins debe generar dos claves matemáticamente relacionadas, una de las cuales se hace pública y otra se mantiene en privado. Si una persona (digamos, «A») quiere transferir la titularidad de un bitcoin a otra persona (digamos, «B»), «A» debe utilizar su clave privada para ordenar

> la transferencia (10) y consignar la clave pública de «B» para identificar al destinatario de la misma. En este contexto, una vez finalizada la operación, se dice que «B» pasa a ser el nuevo titular del bitcoin referido, dado que el sistema sólo permitirá una nueva transferencia del mismo si ella es ordenada mediante la utilización de su clave privada. La clave pública (en el ejemplo referido en el párrafo precedente, la clave pública de «B»), que funciona entonces como una especie de nombre de usuario o de identificación de cuenta, no necesariamente está relacionada con los datos personales de su titular […].

2. Riesgos asociados a la utilización de Bitcoin en materia de lavado de activos

Hemos visto que las criptomonedas disponen de una serie de ventajas que tienen el potencial de transformar la economía mundial. Entre ellas se destacan la descentralización, dado que no está controlado por una autoridad como ser un banco central o un Estado, lo que proporciona grandes márgenes de autonomía.

Se afirma también que el uso de BTC hace posible que dos partes se relacionen directamente entre ellas sin la intervención de un tercero, y que pueden realizarse transacciones en forma rápida independientemente del lugar en el que se encuentren.

El anonimato es otra de las características que se reputan como ventajosas, fundamentalmente para ciertos usuarios legítimamente preocupados por la protección de su privacidad.

Ahora bien, algunas de esas ventajas también las convierten en instrumento para la comisión de delitos que van desde el lavado de activos, el financiamiento del terrorismo, la compraventa de armas y drogas en mercados negros, hasta la estafa y la evasión fiscal.

En particular, al facilitar las relaciones entre clientes no presenciales, el uso de BTC contribuye a la actividad ilegal transfronteriza respecto de espacios locales no regulados o con regulación no homogeneizada. En tales situaciones se torna difícil la adopción de medidas integrales antilavado. Sumado a ello, frente a la comisión de hechos delictivos transfronterizos, seguramente surjan problemas vinculados a la competencia territorial y los derivados de la dispersión de la evidencia.

Los detractores del BTC también advierten que la rapidez de las transacciones se erige como un obstáculo para el monitoreo preventivo de actividades potencialmente ilícitas, lo que a su vez se traduce en una mayor probabilidad de éxito desde la perspectiva de las fases de colocación y encubrimiento de la actividad de blanqueo y en un deterioro considerable de la eficacia de la persecución policial.

A su vez, y dado que el BTC permite mayor anonimato que los métodos tradicionales de pago -ello así, por cuanto las direcciones que funcionan como cuentas carecen de información personal de su titular-, no se generan registros del historial asociados a personas o entidades determinadas, ni las operaciones requieren o proporcionan la identificación de sus reales intervinientes.

Sobre este punto, Navarro Cardoso (2019) afirma que

> […] la propia arquitectura del bitcóin, sustentada sobre la cadena de bloques, permite la trazabilidad de las transacciones, pero ello no conlleva la identificación de los actores reales que intervienen en ella. Es en este contexto en el que hay que situar la afirmación relativa al anonimato de las transferencias y, por ende, la financiación

> anónima. […] Un dato de todo punto revelador del anonimato de bitcóin, de interés...en tanto impide la persecución del blanqueo, es que entes y organismos como la BCE, el GAFI o Europol […] no dudan en reconocerle tal característica. Así mismo, la directora del Fondo Monetario Internacional, F. Lagarde, en el blog de la propia institución, publicó un documento reconociéndolo.

Siguiendo con el desarrollo de este punto, se afirma también que el anonimato en las transacciones imposibilita la aplicación de las medidas antilavado *know your customer* (por sus siglas en inglés, «KYC») y afecta las acciones antiblanqueo que pudieran implementarse en pos de vincular al actor con una operación sospechosa.

En efecto, difícilmente se puedan monitorear transacciones si no se conocen las partes que intervienen en ellas. Una vez más, Navarro Cardoso (2019) nos enseña que, si bien no todas las acciones de monitoreo y detección temprana de actividades sospechosas requieren conocer a los actores, no menos cierto es que, a la hora de imputar un ilícito administrativo y/o penal, será preciso conocer a los sujetos que intervinieron en ellas.

Agrega que ello contribuye decididamente a la tercera fase del delito de lavado de activos -la colocación- «[…] porque, incluso, facilita la actividad de un posible testaferro».

Vinculado lo anterior con la descentralización, la falta de supervisión por un órgano de control deviene en la necesidad de incrementar los sujetos obligados a reportar operaciones sospechosas ya que, de otro modo, las normas antilavado podrían devenir completamente inútiles.

Por otro lado, si bien existen desarrollos informáticos que permiten cierto nivel de monitoreo e identificación de este tipo de operaciones, se ha propiciado el desarrollo de herramientas y servicios adicionales de anonimato, que dificultan aún más el seguimiento de las transacciones y el origen de los fondos, y se conocen como anonymiser.

En su documento *directrices para un informe basado en riesgo (sobre) monedas virtuales* (2015), el GAFI dice que el término *anonymiser* «[…] se refiere a las herramientas y servicios, tales como acuñado y mezcladores, diseñados para ocultar la fuente de una transacción de Bitcoin y facilitar el anonimato».

En dicho documento también encontramos una definición del mixer o mezclador:

> […] es un tipo de anonymiser que oscurece la cadena de transacciones en los blockchain mediante la vinculación de todas las transacciones en la misma dirección bitcoin y enviarlas juntas de una manera que les hace parecer como si fueron enviadas desde otra dirección. Un mezclador o tumbador envía las transacciones a través de una serie de transacciones no reales complejas, semi-al azar que se le hace extremadamente difícil vincular monedas virtuales específicas (direcciones) con una transacción determinada. Servicios de mezclador funcionan con el recibo de instrucciones de un usuario para enviar fondos a una dirección bitcoin particular. El servicio de mezclado entonces 'mezcla' esta transacción con otras transacciones de usuarios, tal que llega a ser confuso a quien el usuario pretendía enviar los fondos. (Ejemplos: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Algunos recurren a coinjoin, que también es una herramienta de privacidad y que permite agrupar transacciones de múltiples usuarios en una única transacción combinada, de manera que los detalles específicos de quién envió bitcoins a quién se vuelvan difíciles de rastrear.

Para ello, los usuarios encuentran una manera de coordinarse (a menudo a través de un servicio específico o un protocolo) para realizar una transacción conjunta, en la que cada uno pretende enviar una cierta cantidad de BTCs a una o más direcciones.

Luego combinan -mezclan- sus entradas -las direcciones desde donde se envían los BTC- y salidas -donde serán enviadas- en una sola transacción CoinJoin, y cada usuario firma su parte, aprobando así la porción de la operación que le corresponde.

Firmada la transacción, esta se transmite a la red de BTC y se confirma como cualquier otra.

Otro mecanismo de anonimato es recurrir al uso de direcciones y carteras desechables -por cada transacción se crea una nueva dirección de BTC con el fin de evitar que se acumulen patrones que puedan ser analizados para rastrear su actividad- o de redes TOR y VPNs -que permiten ocultar la dirección IP, lo que hace aún más difícil la vinculación de una dirección de Bitcoin con una identidad específica basada en la información de la red-.

A modo de conclusión, y nuevamente con cita de Navarro Cardoso (2019), «[a] partir de lo expuesto podríamos afirmar que las características propias de la blockchain de BTC favorece su uso delictivo. Si a ello se le suma el incremento de anonimato que ofrecen los mezcladores y carteras oscuras, el riesgo del BTC como instrumento de blanqueo se dispara».

a. Impacto de los criptoactivos en esta particular modalidad delictual

i. *Aspectos relevantes del delito de lavado de activos*

A modo introductorio, conviene recordar que el término lavado de activos -en inglés, *money laundering*- se habría originado en los EE.UU., en la década de 1920, a partir de la necesidad de describir el proceso mediante el cual los grupos criminales organizados -la mafia- ocultaban el origen de los fondos ilegítimamente obtenidos mediante la compra de negocios como lavanderías, que utilizaban para darles apariencia de legalidad.

En efecto, las lavanderías manejaban grandes volúmenes diarios de dinero en efectivo, lo que las hacía ideales para mezclar el dinero obtenido ilegalmente con los ingresos legítimos que se percibían.

Ahora bien, el lavado de activos irrumpió en la escena global a partir del desembarco del narcotráfico como problema transnacional. A inicios de la década del 70 se implementó en los EE.UU. una rigurosa política regulatoria que exigía a las entidades financieras que reportaran determinadas transacciones que se realizaban mediante la prestación de sus servicios.

Luego, en los años '80, concretamente en el año 1986, EE.UU. incorporó el lavado de activos al catálogo de delitos penales en procuras de obtener una sanción punitiva que incluyera no sólo a los actores de la cadena de producción, distribución y venta de sustancias estupefacientes, sino también a los encargados de la colocación de su producido.

En 1988 esta tipificación se internacionalizó con la firma de la Convención de Viena y en los años venideros se firmaron numerosos acuerdos internacionales en gran cantidad de países que incluían varios delitos, entre ellos el lavado de activos.

A nivel local, el primer antecedente legislativo en la materia lo encontramos en la ley 23.737 (1989) sobre el régimen legal de estupefacientes, que en su art. 25 reprimía con pena de 2 a 10 años de prisión y multa de 6 a 15 mil australes al que

> […] sin haber tomado parte ni cooperado en la ejecución de los hechos previstos en esta ley, interviniere en la inversión, venta, pignoración, transferencia o cesión de las ganancias, cosas o bienes provenientes de aquéllos, o del beneficio económico obtenido del delito siempre que hubiese conocido ese origen o lo hubiera sospechado.

Con igual pena castigaba al «[…] que comprare, guardare, ocultare o receptare dichas ganancias, cosas, bienes o beneficios conociendo su origen o habiéndolo sospechado».

Culminaba señalando que, a los fines de la aplicación de dicho artículo, «[…] no importará que el hecho originante de las ganancias, cosas, bienes o beneficios se haya producido en el territorio extranjero», haciéndose eco del carácter transnacional del narcotráfico.

La evolución legislativa culminó con la actual redacción del art. 303 del código penal argentino, que reprime

> […] con prisión de tres (3) a diez (10) años y multa de dos (2) a diez (10) veces del monto de la operación, el que convirtiere, transfiriere, administrare, vendiere, gravare, adquiriere, disimulare o de cualquier otro modo pusiere en circulación en el mercado, bienes u otros activos provenientes de un ilícito penal, con la consecuencia posible de que el origen de los bienes originarios o los subrogantes adquieran la apariencia de un origen lícito […].

Dicho lo anterior, existe consenso generalizado en cuanto a que el delito de lavado de activos se divide en tres etapas: colocación, estratificación e integración. La primera consiste en introducir los fondos ilegales en el sistema financiero; en la segunda se procura separar aún más el dinero ilícito de su origen mediante la realización de múltiples y diversas transacciones diseñadas para dificultar el seguimiento del dinero; en la fase final, los fondos blanqueados se integran de nuevo en la economía legítima.

Sin embargo, tal división muchas veces resulta irreconocible, dado que las fases pueden superponerse, en ocasiones son simultáneas o desordenadas, ello como consecuencia de la utilización de medios de blanqueo cada vez más complejos.

Ahora bien, con respecto a la fase de colocación, Carrizo (2003) nos dice que:

> Se considera a esta etapa la más delicada del proceso de lavado, atento a que es aquí cuando el lavador opera los mecanismos a su alcance a los fines de lograr la reducción de los bienes de extraño origen, que rara vez pueden justificar y, de este modo lograr una manipulación de dichos bienes de manera subrepticia. Cuando hablamos de reducción del bien, nos estamos refiriendo no a una quita o pérdida de su valor, sino a la maniobra llevada a cabo por el lavador a los fines de convertir, cambiar o sustituir el bien indicado para así poder continuar con el proceso sin que pueda ser detectado por la autoridad.

Sobre la fase de estratificación, Valdés Trapote (2022) aporta:

> […] consiste en la mezcla del dinero o los bienes en diversas empresas e instituciones financieras. El dinero se transporta a otros lugares para ocultar su origen ilícito. Lo importante aquí es adquirir activos para transferirlos o intercambiarlos con otros de

> origen lícito. En esta etapa, una vez que el dinero entra en los circuitos financieros, se hacen movimientos para ocultar su origen, con el fin de erradicar cualquier posible vínculo entre el dinero colocado y su origen. Las técnicas más frecuentes son enviar el dinero a paraísos fiscales o centros offshore, para asegurar que los fondos circulen a través de diferentes países, instituciones y cuentas mantenidas por diferentes personas físicas o jurídicas

Finalmente, recurriendo a Marengo (2011), la integración es el

> […] último escalón en el proceso del lavado. Se busca con esta fase el perfecto asentamiento de los bienes y […] que […] las autoridades consideren que ellos fueron obtenidos por medios legítimos y que pertenecen de manera definitiva a la economía oficial. Al haber transcurrido sin inconvenientes las etapas anteriores y dejado constancia de ello a través de registros contables y tributarios se les otorga apariencia legal, de modo de enervar cualquier tipo de persecución.

Toda vez que no pretendemos analizar a fondo el tipo penal del art. 303 del código de fondo -por no ser objeto de la presente investigación-, nos limitaremos a señalar que

- la acción punible podría definirse como la transformación de bienes que provienen de un delito y otorgarles apariencia de licitud
- sujeto activo del delito puede ser cualquier persona
- el ilícito penal al que hace referencia el art. mencionado debe interpretarse como comprensivo de la totalidad de los delitos del C.P. y las leyes especiales, y también las infracciones de naturaleza penal aduaneras, cambiarias o fiscales
- en cuanto al delito precedente, la Convención de Varsovia establece como requisito para una condena por blanqueo de capitales que existe una condena previa o simultánea por aquella primera infracción
- el tipo subjetivo solo admite el dolo directo debido a que hace falta que el sujeto conozca que los bienes provienen de la comisión de un hecho delictivo y su intención de concretar el fin de apariencia exigido por la norma.

ii. *Criptolavado de activos como forma específica de esta modalidad criminal.*

Sentado cuanto precede, diremos que el criptolavado -esto es, el recurso al uso de activos virtuales (AV) para el lavado de activos- es una derivación natural del surgimiento de los mercados de bienes y servicios ilícitos en la denominada *dark web*, un sector de la Internet al que solo se puede acceder mediante la implementación de herramientas tecnológicas que permiten navegar anónimamente, como el sistema TOR.

Es, a su vez, consecuencia de la aparición de Bitcoin, que posibilitó el funcionamiento de estos mercados oscuros al ofrecer un medio de pago, en principio, también anónimo.

El primero de esos mercados fue Silk Road, que a pesar de haber sido cerrado con bastante rapidez por las autoridades -inició en enero del año 2011 y para octubre del año 2013 el FBI ya había cerrado el sitio y arrestado a su propietario Ross Ulbritch, quien terminó condenado a cadena perpetua en 2015-, fue inmediatamente reemplazado con otros similares, que hoy son fuente de un alto porcentaje de los fondos ilícitos que se reciclan mediante los activos virtuales y los servicios asociados a éstos.

Sobre este punto, el GAFILAT (2021) explica que «un estudio que analizó las transacciones con Bitcoin entre 2013 y 2016 concluyó que la casi totalidad de los bitcoins de origen ilícito lavados a través de plataformas de intercambio de criptomonedas provenían de los mercados de la Red oscura».

Ahora bien, este mismo proceso de tres etapas descripto en relación al lavado de dinero se aplica también a los criptoactivos, pero las complejidades asociadas a cada fase son inherentemente distintas.

Al respecto, el GAFILAT (2021) sostiene

> El proceso de 'criptolavado' admite las mismas tres etapas que el lavado de activos tradicional (colocación, estratificación e integración). Sin embargo, las maniobras asociadas a cada una de esas fases tienen características propias, producto de la naturaleza de los AV involucrados. Así, por ejemplo, la propia necesidad de que exista, o no, una etapa de colocación depende de si los fondos ilícitos son obtenidos en moneda fiduciaria o directamente en criptomonedas. Ello así, desde que en el primer supuesto es necesario efectuar una conversión de una moneda a otra, mientras que en el segundo no lo es.

En sentido similar, Valdés Crapote (2022) nos enseña

> Por ejemplo, en la etapa de colocación, los fondos se mueven de un banco tradicional a una cuenta con un servicio de cambio de criptoactivo con el fin de comprar monedas primarias como bitcoin o Ethereum. Luego, en la fase de capas, las monedas primarias se intercambian por varios criptoactivos, alternativos, que permitan mayor privacidad, en un intento de enturbiar el papel electrónico, lo que hace más difícil para las fuerzas del orden seguir el rastro de dinero. Este proceso también se conoce como salto de cadena. Luego, en la etapa de integración el lavador puede cambiar esos criptoactivos de nuevo a otros activos más conocidos, que luego se pueden cambiar de nuevo por dinero tradicional. Mientras que la descripción es de nuevo demasiado simplificada, el relato pretende describir un esquema bien diseñado pues, al fin y al cabo, las criptomonedas han sido vistas como una oportunidad de inversión única y lucrativa, no solo con el fin de lavar activos. Como resultado, puede ser difícil detectar la identificación de actividades de colocación o el reconocimiento de una transacción sospechosa iniciada a través de un intercambio de criptomonedas y deslindarla de una rápida y fácil inversión. Esto es especialmente complejo si la criptomoneda intercambiada no tiene suficientes protocolos de conocimiento de su cliente y favorece el anonimato.

Por su parte, Donna (2022) sostiene que el tipo penal del art. 303 no encontraría ningún inconveniente en cuanto a su aplicación, «ya que el dinero con el que se compra Bitcoins o cualquier pago con criptomoneda debe provenir de un ilícito, si se da ese requisito entra en el tipo penal de lavado de argentina».

Continúa por señalar que

> El problema podría aparecer en la instrucción, en el sentido de si...el poder judicial cuenta con las herramientas, los medios y personas capacitadas en programación, sistemas financieros, etc. (entendiendo que ya tiene gente capacitada en Derecho penal) a los fines de poder recaudar la información o la prueba necesaria para probar el ilícito o prevenirlo. En otras palabras, el tipo penal es el mismo de siempre, lo que se vuelve más complejo son los métodos que se utilizan para llevar a cabo la negación al Derecho, ello exige mayor conocimiento en sistemas informáticos, en fianzas, etc.

Profundizando en las características asociadas a las etapas del criptolavado, hemos de mencionar que en la colocación se suele recurrir a un *proveedor de servicios de activos virtuales* (en adelante, «PSAV»), por lo general una plataforma de intercambio de criptomonedas que permita convertir la moneda fiduciaria en Bitcoins.

Además, en jurisdicciones que han ajustado su normativa a lo establecido en la Recomendación 15 del GAFI, que exige a los PSAV el reporte de operaciones

sospechosas de sus clientes, los lavadores podrían optar por utilizar un PSAV ubicado en un país/Estado que no esté sometido a deberes de ALA o que incumpla sus obligaciones.

Concluida la etapa de colocación, los delincuentes pueden recurrir a múltiples mecanismos para la estratificación de los fondos. Por un lado, se pueden realizar múltiples transacciones entre monederos de activos virtuales controlados por una misma persona -tengamos en cuenta que las criptomonedas admiten a los usuarios mantener un número indefinido de direcciones- o por varios sujetos distintos, lo que sumado a la simplicidad de creación de nuevas direcciones, la disociación con la identidad real del usuario, la velocidad de las transacciones y la facilidad con la que se pueden cruzar fronteras nacionales y regulatorias, hacen posible la creación de patrones de estratificación extremadamente complejos.

Tiene dicho el GAFI (2021) que

> Los PSAV cumplen una función esencial en los esquemas de criptolavado, ya sea en la fase de colocación (para la conversión de moneda fiduciaria en AV), durante la fase de estratificación (por ejemplo, permitiendo el cambio de una criptomoneda por otra o brindando servicios de «mezclado») o en la etapa final, donde los/las beneficiarios/as de la maniobra convierten los fondos nuevamente a moneda fiduciaria. Ello ha derivado en la aparición de plataformas de intercambio de AV específicamente creadas y estructuradas para facilitar el criptolavado. En tal contexto, un informe reciente concluye que un tercio del volumen de tráfico transfronterizo de bitcoins se vuelca a PSAV con políticas deficientes de ALA/CFT.

Entre los principales servicios que ofrecen los PSAV a los delincuentes encontramos los de mezclado o mixing de criptomonedas, que combinan los ingresos y egresos de fondos de distintos/as usuarios/as para tornarlos indistinguibles entre sí.

También pueden implementarse, a través de los PSAV, otras metodologías de estratificación, como el chainhopping, que significa salto de cadenas y que consiste, básicamente, en el intercambio de diferentes criptomonedas entre sí, con la finalidad de cortar la cadena de transacciones en las respectivas blockchain.

3. Modalidades de lavado de activos mediante el uso de criptomonedas

A continuación, haremos una breve reseña de las acciones y estrategias más comúnmente utilizadas en materia de lavado de activos a través de criptomonedas.

Conviene recordar aquí que las criptomonedas no son ilícitas en sí mismas, tampoco lo es la tecnología que les sirve de soporte, sino el fin o uso que le dan quienes se dedican a la actividad criminal.

a. Compra de criptomonedas

La compra de criptomonedas puede ser un método para lavar dinero. Así lo afirma Navarro Cardoso (2019), y agrega: «El sujeto interesado en la adquisición de alguna de ellas ofrece dinero fiduciario a cambio de recibir criptomoneda. La colocación misma de esta puede ser una operación de lavado (recordando...que la segunda fase del blanqueo, el encubrimiento, o se entiende innecesaria en tanto implícito en la opacidad de la blockchain del bitcóin, o se produce con el recurso a los mezcladores)».

b. Monetización o tokenización

Las monedas digitales no necesariamente tienen que cambiarse por monedas legalmente establecidas, sino que pueden ser utilizadas directamente o a través de un proveedor de servicios de custodia de monederos electrónicos para la adquisición de bienes y servicios. De allí, entonces, la posibilidad de destinar activos obtenidos ilegítimamente con fines lícitos.

En opinión que compartimos, y con cita -una vez más- del autor Navarro Cardoso (2019), ha de señalarse que:

> La innecesariedad de la monetización va en parte ligada, como resulta obvio, a la generalización del uso de estas criptodivisas, sea bitcóin, o la que resulte triunfante en esta también competición, pues existen alternativas con mayores ventajas desde el punto de vista del uso delictivo para blanquear dinero.

Por su parte, la expresión *token*, en el ámbito tecnológico, remite a la idea de *ficha*, *cupón* o *vale*, pues su uso permite el acceso a un bien o un servicio. En general, los criptotokens, si bien guardan similitud con las criptomonedas -en cuanto son una unidad de valor aceptada por una comunidad y se sustentan en teconología de cadena de bloques-, tienen más funcionalidades -como ser ceder un derecho, abonar un trabajo, permitir acceso a servicios extras de la empresa que lo ha emitido-, que les son asignadas por la entidad privada que las emite.

Por ello se afirma que existe una tendencia hacia la *tokenización*, proceso que facilita en mucho la actividad de blanqueo, empleando los bitcóin como moneda y como activo financiero.

c. Minado de criptoactivos

En este caso, los delincuentes invierten dinero obtenido ilícitamente en equipos de minería de criptomonedas que pueden incluir hardware especializado como ASICs (Application-Specific Integrated Circuits) o GPU (Graphics Processing Units). La compra de equipos de minería es una forma de convertir dinero en efectivo en bienes tangibles que no están directamente ligados a actividades ilícitas.

Una vez adquiridos los equipos, los delincuentes operan una instalación de minería para generar criptomonedas (como Bitcoin, Ethereum, etc.) que luego pueden vender en *exchangers* -plataforma (en línea o física) que permite a los usuarios comprar, vender e intercambiar criptomonedas por otras criptomonedas o por monedas fiduciarias (como dólares, euros, yenes, etc.)-, que tienen regulaciones más laxas o que no implementan estrictos procedimientos de Conozca a Su Cliente (KYC).

En consonancia con ello, Valdés Crapote, A. (2022) afirma que «[e]xisten organizaciones que obtienen dinero ilícito a través de diversas actividades delictivas y necesitan blanquearlo, usar ese dinero para comprar equipo minero, con el fin de minar criptoactivos. Una vez que los beneficios se obtienen a través de la minería, podrían reinvertirse en cualquier activo o en una actividad aparentemente legal, cuyos beneficios pueden justificarse ante las autoridades».

d. Exchangers

Como ya dijimos, un *exchanger* de criptomonedas, también conocido como intercambio o casa de cambio de criptomonedas, es una plataforma (en línea o física) que permite a los usuarios comprar, vender e intercambiar criptomonedas por otras criptomonedas o por monedas fiduciarias (como dólares, euros, yenes, etc.).

Estas plataformas juegan un papel crucial en el ecosistema cripto, dado que proporcionan la estructura necesaria para que los usuarios puedan acceder, comerciar y utilizar criptomonedas.

Ahora bien, ¿cuáles son los riesgos asociados a los *intercambios* s en materia de lavado de activos? Una vez más, Valdés Crapote (2022) nos acerca la respuesta, afirmando que son tres: el primero, que tradicionalmente no han sido sujetos obligados en cuanto a la prevención del blanqueo de capitales, aunque las legislaciones más modernas vienen modificando este paradigma imponiendo su inscripción en registros concretos, con obligaciones parecidas a los bancos; el segundo, que los mandantes no operan desde el país en el que está radicada la plataforma; y el último, que pueden ser controladas directamente por una organización criminal que se dedique precisamente al blanqueo de capitales».

e. Traders

Un trader es una persona que compra y vende criptomonedas con el objetivo de obtener beneficios financieros, sirviéndose de la volatilidad del mercado para realizar transacciones en diversos intervalos de tiempo, desde minutos hasta meses, según su estrategia y estilo de trading.

En general, se anuncian principalmente a través de la darkweb para cambiar moneda virtual por monedas fiduciarias.

En torno al tópico que nos convoca, Valdés Crapote, A. (2022) sostiene que existen algunos indicadores que podrían vincular el trading con el blanqueo de capitales, entre las cuales menciona:

- Operar con moneda virtual a partir de efectivo en volúmenes significativos.
- Realizar cambios de moneda virtual con efectivo utilizando canales que implican pagar altas comisiones y/o soportar peores tipos de cambio que los métodos alternativos.
- Intercambios hechos en lugares inusuales y anónimos. En muchos casos, las ventas y compras se organizan a través de foros de Internet (p2p) y los intercambios tienen lugar físicamente para garantizar que el comprador de las criptomonedas paga en efectivo y el vendedor simplemente proporciona su contraseña de cuenta.
- La compra se realiza con beneficios directos de otras actividades ilícitas.

f. BTMs o cajeros automáticos de criptomonedas

Los cajeros automáticos de criptomonedas (Bitcoin ATMs o BTM) son dispositivos físicos que, mediante el uso de dinero de efectivo o tarjetas bancarias, permiten la compra y, en algunos casos, la venta de criptomonedas como Bitcoin, Ethereum, Litecoin y otras.

Los BTM suelen encontrarse en tiendas abiertas al público y normalmente no son objeto de licencia, por lo que sus medidas de instalación, mantenimiento y seguridad no están reguladas ni supervisadas por ningún organismo público.

De hecho, dependiendo de las regulaciones locales, algunos cajeros automáticos de criptomonedas permiten transacciones anónimas o con requisitos mínimos de verificación de identidad, lo que aumenta el riesgo de lavado de activos.

A partir de lo expuesto, deviene ineludible preguntarnos cómo podría lavarse dinero mediante el uso de este tipo de dispositivos. Para dar respuesta a dicho interrogante recurrimos a Adra, R. (2021), quien afirma:

> […] el lavado comienza a partir de la creación de varias cuentas de Bitcoin, cuyo único requisito es dar una cuenta de correo electrónico. El criminal crea varias, sin correlación con su verdadera identidad. Luego pide que el intercambio se haga por medio de este criptoactivo, pero depositando los bitcoins a diferentes cuentas con montos pequeños. Como segunda etapa, el retiro del dinero en efectivo lavado se hace de a poco, tomándolo de las distintas cuentas. En general, se hace por interpósitas personas, las cuales se van a encargar de retirarlo, para no despertar sospechas.

En sentido concordante, Hyman M. (2015) pone el ejemplo de un narcotraficante que crea varias cuentas de Bitcoin, y ya que el único requisito para abrir una cuenta de Bitcoin es proporcionar un correo electrónico, este narcotraficante crea un correo electrónico que no corresponde con su verdadera identidad por cada cuenta de Bitcoin. A raíz de esto exige a sus compradores que paguen las transacciones en bitcoins a diferentes cuentas en montos pequeños (esto para no levantar sospechas). A continuación, el narcotraficante utiliza una red de «mulas» que van a sacar poco a poco dinero en efectivo de las diversas cuentas de Bitcoin que posee. Adicionalmente puede hasta convertir sus ganancias en bitcoin en otras criptomonedas para encubrir aún más sus operaciones delictivas.

g. Mixers o Tumblers

Los «mezcladores» o «conmutadores» («mixers» o «tumblers») funcionan como servicios independientes de lavado de activos. El paso por un mixer sustituye la transferencia de AV entre dos direcciones (por ejemplo, de Bitcoin), de modo tal que los fondos de origen ilícito que una persona pretende transferir a otra se entremezclan con los provenientes de muchas otras direcciones de AV antes de ser finalmente enviadas a la del/la destinatario/a, dificultando la identificación de la dirección de origen y de las cuentas asociadas con los fondos de origen ilícito.

En términos más sencillos, según afirma Oppel, S. (2022):

> La manera de operar de este tipo de plataformas es muy sencilla. Recibe por parte de los usuarios una determinada suma de bitcoins y les devuelve el mismo monto -restando, obviamente, el cobro de una determinada comisión-, pero distribuido en varias operaciones y utilizando para ello sumas que fueron depositadas por otros usuarios. Así, cruza los saldos y los re-integra de manera 'partida' a través de varias

> transacciones, tornado prácticamente imposible poder trazar un seguimiento de ellos.

Los mixers funcionan de manera similar a un FCI, en donde múltiples individuos acumulan sus fondos para obtener un beneficio colectivo. La diferencia radica en que, en el caso de los mezcladores, el fondo común es utilizado para concretar múltiples transacciones con criptomonedas, y el beneficio es lograr un mayor grado de anonimato impidiendo la vinculación de las transferencias con direcciones de AV específicas.

En general, los mixers que se dedican al lavado de activos, amén de cobrar una comisión por sus servicios, no guardan registro de usuarios e incluso pueden opacar su infraestructura operando como servicios ocultos en TOR.

h. Chainhopping

El chainhopping es una técnica utilizada para mover criptomonedas de una blockchain a otra, a menudo a través de puentes (bridges) o intercambios descentralizados.

Los bridges son protocolos que permiten transferir criptomonedas y activos virtuales entre diferentes blockchains, facilitando la interoperabilidad y permitiendo a los usuarios mover sus activos de una red a otra sin necesidad de intermediarios centralizados.

Por su parte, los DEX o intercambios descentralizados son plataformas que permiten a los usuarios intercambiar criptomonedas directamente entre ellos, sin la necesidad de una autoridad central, lo que también ayuda a mantener el control sobre sus fondos. Ambos mecanismos son clave para la flexibilidad del ecosistema cripto, pero también presentan riesgos en términos de seguridad y lavado de activos.

Estos mecanismos permiten dispersar los activos entre diferentes redes, lo que a su vez dificulta el rastreo de las transacciones y posibilita a los delincuentes ocultar el origen ilícito de los fondos.

4. Casos de lavado de activos mediante el uso de criptomonedas. Dificultades y desafíos.

a. Silk Road (EEUU)

Silk Road fue un mercado en línea fundado en 2011 por Ross Ulbricht, conocido como «Dread Pirate Roberts», donde se podían comprar y vender drogas ilegales, armas, información de identidad robadas y otros bienes y servicios ilegales mediante el empleo de Bitcoins.

El GAFI (2015) explica que:

> «…funcionaba como un ciber bazar global de mercado negro que intermediaba transacciones criminales anónimas y fue utilizado por varios miles de narcotraficantes y otros vendedores ilegales para distribuir bienes y servicios ilegales a más de cien mil compradores, un tercio de los cuales se cree que estaban en los Estados Unidos».

Se estima que facilitó transacciones por alrededor de 1.200.000.000 USD, las cuales le significaron a Ulbritch un aproximado de entre 10 y 15 millones de dólares durante el

tiempo que el sitio estuvo operativo, principalmente a través de comisiones que percibía por las transacciones realizadas.

La moneda exclusiva de intercambio en este particular mercado de bienes y servicios ilegales era el Bitcoin, lo que permitió a compradores y vendedores ocultar su identidad, a la vez que podían obtener un número ilimitado de direcciones Bitcoin y utilizar una diferente para cada operación dificultando aún más el rastro de los activos obtenidos ilícitamente.

Profundizando en el funcionamiento de Silk Road, y nuevamente con cita del GAFI (2015), diremos que:

> El sistema de pago de Silk Road funcionaba como un banco interno de Bitcoin, donde cada usuario de Silk Road tenía que tener una cuenta para realizar transacciones en el sitio. Cada usuario de Silk Road tenía al menos una dirección de Silk Road de Bitcoin (y posiblemente miles) asociada (s) a la cuenta de Silk Road del usuario, almacenadas en carteras mantenidas en servidores controlados por Silk Road. Para realizar una compra, un usuario obtenía bitcoins (normalmente a través de un cambiador de Bitcoin) y lo enviaba a una dirección Bitcoin asociada a su cuenta de Silk Road para financiar la cuenta. Cuando se hacía una compra, Silk Road transfería los bitcoins del usuario a una cuenta de fideicomiso que mantenía, en espera de la finalización de la transacción y luego se transfería los bitcoins del usuario/comprador de la cuenta de fideicomiso a la dirección de Bitcoin Silk Road del vendedor. Como un paso adicional, Silk Road empleaba a un 'tumbador' para cada compra, que…enviaba todos los pagos a través de una serie compleja, semi-random de transacciones dummy […].

Principales desafíos que implicó el caso.

El caso Silk Road fue -y sigue siendo- un ejemplo emblemático de cómo las criptomonedas, especialmente Bitcoin, pueden ser utilizadas en actividades ilegales. Los principales retos que implicó el caso se vinculan con:

- *Anonimato*. Si bien las transacciones de Bitcoin son públicas y quedan registradas en la cadena de bloques, los usuarios podían operar de manera relativamente anónima dado que no era necesario brindar información personal para crear una billetera, lo que facilitaba el comercio de bienes y servicios ilegales ofrecidos en Silk Road.
- *Dificultad de rastreo*. Aunque las transacciones eran visiles, como ya dijimos, rastrear la identidad de los usuarios resultaba complejo dado que utilizaban técnicas de como «mixers» o «tumblers» para ocultar el origen de los fondos.
- *Mercados oscuros*. La moneda de cambio exclusiva para operar en Silk Road era el Bitcoin, lo cual demostró la capacidad de las criptomonedas para facilitar las transacciones en el mercado negro.

b. BTC-e (EEUU)

El primer caso del que nos ocuparemos es el de BTC-e, una plataforma de intercambio de criptomonedas que operó entre 2011 y 2017 y fue objeto de investigaciones por su presunta implicación en el lavado de dinero y actividades ilícitas a gran escala.

El operador de BTC-e era un ciudadano ruso llamado Alexander Vinnik, quien luego de ser arrestado en Grecia en el año 2017 y de transitar un largo proceso de extradición, se declaró culpable de un cargo de conspiración para cometer lavado de dinero en los EEUU.

Según la acusación formulada en su contra, BTC-e no se registró como una empresa de servicios monetarios en los EE. UU., no aplicó ninguna regla de conocimiento del cliente o contra el lavado de dinero y no recopiló ningún dato de los clientes, utilizando empresas fantasmas para procesar conversiones fiduciarias para BTC-e.

En cuanto al modus operandi, la plataforma funcionaba con una mínima verificación de identidad, dado que para abrir una cuenta solo se requería un nombre, una dirección de correo electrónico y una contraseña, lo que facilitaba el anonimato. La plataforma no permitía a los usuarios transferir fondos directamente desde sus cuentas bancarias, sino que utilizaba intermediarios, lo que complicaba el rastreo de las transacciones. Esta estructura ayudó a los delincuentes a ocultar el origen de los fondos y dificultó que las autoridades financieras detectaran actividades sospechosas.

Ampliando este punto, Linares Quintana, B. (2019) indica que:

> el usuario debía crearse una cuenta para acceder al sitio web y una vez que la fondeaba con activos se encontraba en condiciones para realizar una transacción (cambiar criptomonedas a moneda fiat o viceversa), o simplemente para almacenar en dicha cuenta los activos virtuales.
>
> […] El usuario de BTC-e no podía fondear su cuenta mediante una transferencia bancaria (desde su cuenta bancaria) a (una cuenta bancaria de BTC-e) sí mismo, sino que debía hacerlo a (una cuenta bancaria) alguna sucursal o entidad afiliada de BTC-e. Tampoco podía extraer fondos directamente desde su cuenta, sino que debía requerir un depósito o una extracción por medio de otro exchanger, de manera que BTC-e evitaba recolectar cualquier información de los usuarios por la realización de transferencias bancarias o de cualquier otra actividad que dejara rastro en el sistema financiero tradicional.

Principales desafíos que presentó el caso BTC-e.

El caso BTC-e presentó varios desafíos para las autoridades y los investigadores debido a la naturaleza de las criptomonedas y a la estructura de la plataforma. Entre ellos podemos mencionar:

- *Anonimato y falta de regulación*. BTC-e operaba sin cumplir con las normativas de «conoce a tu cliente» (know your customer - KYC) y «anti-lavado de dinero» (Anti Money Laundering - AML). Esto permitía a los usuarios abrir cuentas con solo un nombre, una dirección de correo electrónico y una contraseña, sin requerir verificación de identidad, lo que dificultaba no sólo la individualización de los usuarios sino también rastrear las transacciones, permitiendo a los delincuentes operar con mayor facilidad.
- *Alcance de la operación*. BTC-e era una plataforma internacional con usuarios en todo el mundo, lo que implicaba la coordinación de diversas agencias y jurisdicciones. El arresto del operador de BTC-e, Alexander Vinnik, se realizó en Grecia, pero involucró a autoridades de Estados Unidos y varios otros países. La falta de armonización entre regulaciones de diferentes países complicaba la investigación y el procesamiento.
- *Uso de criptomonedas y mixers*. La plataforma permitía a los usuarios lavar dinero utilizando criptomonedas, que pueden ser difíciles de rastrear. Además, BTC-e facilitaba el uso de servicios de mezcla de criptomonedas («mixers») que fragmentaban y combinaban transacciones de diferentes usuarios, ocultando el origen y el destino de los fondos.

- *Tecnología avanzada*. Los criminales que utilizaban BTC-e aprovechaban el anonimato y la falta de transparencia de las criptomonedas. Esto requería que los investigadores emplearan herramientas tecnológicas sofisticadas para rastrear las transacciones y descifrar el rastro de los activos ilícitos, lo que ralentizaba el progreso de la investigación.
- *Jurisdicciones offshore*. BTC-e estaba registrada en jurisdicciones offshore, que generalmente tienen regulaciones financieras menos estrictas. Esto complicaba el acceso a información crucial para la investigación y permitía que la plataforma evitara cumplir con regulaciones internacionales de intercambio de criptomonedas.
- *Retiro y depósitos indirectos*. BTC-e evitaba que sus usuarios depositaran y retiraran fondos directamente desde o hacia cuentas bancarias tradicionales. En su lugar, los fondos se canalizaban a través de terceros, como afiliados o otros exchangers, lo que complicaba el seguimiento del dinero.

c. Caso bobinas blancas (argentina)

En el marco de esta causa se secuestró el cargamento de cocaína más grande de la historia del país, aunque la novedad radicó en que fue condenado un operador de criptoactivos por lavar el dinero de la organización criminal.

El operador ofrecía servicios de compraventa de bitcoins por fuera de las plataformas de intercambio, es decir, recibía criptomonedas a una cuenta en el extranjero y entregaba el equivalente en efectivo en el país, o bien recibía dinero en el país y transfería los bitcoins a un beneficiario en el exterior.

En este contexto, las autoridades consideraron que el operador no podía desconocer el origen ilícito del dinero y, por tanto, entendieron que con la prestación de este servicio contribuyó al blanqueo de fondos provenientes del narcotráfico.

La operatoria con Bitcoins:

- el operador de criptoactivos recibía transferencias de divisas de parte de integrantes de la organización criminal que se encontraban en el exterior, destinadas a los integrantes de esa organización que se hallaban en el país, mediante transacciones realizadas en la moneda virtual bitcoin;
- aprovecharon la falta de un organismo de control que regule la operatoria, y la ventaja de que las operaciones resultaran difícilmente asignables a una persona en particular, todo lo cual diluía toda posible trazabilidad para establecer el origen y destino del dinero;
- esa posibilidad de transferir dinero desde el exterior por fuera del sistema bancario y el anonimato de los intervinientes resultaron circunstancias que fueron claramente aprovechadas por la organización criminal;
- el operador recibió las distintas acreditaciones de bitcoins desde un bitcoin address desconocida, pero por orden de un tercero, y fue el operador quien posteriormente entregó su equivalente en dólares a distintas personas de nacionalidad extranjera, quienes se identificaron mediante la exhibición de un billete con una numeración específica.

Principales dificultades evidenciadas en el caso «bobinas blancas».

El caso «bobinas blancas» presentó numerosas dificultades específicas en materia de lavado de activos, dado que los narcotraficantes emplearon métodos complejos para ocultar y blanquear los fondos provenientes del tráfico de cocaína.

Entre ellas podemos mencionar:

- *Estructuración compleja del esquema de lavado*. Los delincuentes utilizaron múltiples capas de empresas de fachada, cuentas bancarias en diferentes jurisdicciones y otros intermediarios para mover y disimular el origen ilícito de los fondos. Estas estructuras, diseñadas para enmascarar el rastro del dinero, complicaban el rastreo de los activos desde su origen hasta su destino final.
- *Uso de criptomonedas*. El uso de criptomonedas para lavar los ingresos del narcotráfico representó una barrera significativa. Las criptomonedas permiten transacciones transnacionales rápidas y, a menudo, anónimas, lo que dificultaba el rastreo de los activos ilícitos, especialmente cuando se usaban servicios de mezcla (mixers) o criptomonedas enfocadas en la privacidad, como Monero.
- *Falta de cooperación internacional*. Si bien hubo coordinación entre países como Argentina, Estados Unidos y Europa, en algunas ocasiones las diferencias entre sistemas legales, así como la falta de tratados efectivos de cooperación en ciertas jurisdicciones, dificultaron el intercambio rápido de información y la identificación de los activos que habían sido transferidos a otras partes del mundo.
- *Metodologías sofisticadas de ocultamiento*. Además de usar criptomonedas, los narcotraficantes emplearon una combinación de bienes físicos (bobinas de acero) y movimientos financieros disimulados para lavar grandes cantidades de dinero. Las técnicas de ocultamiento sofisticadas y diversificadas dificultaban identificar las transacciones ilícitas entre las operaciones legales.
- *Fragmentación de los fondos*. Los delincuentes utilizaron tácticas de fragmentación de los fondos («smurfing»), dividiendo grandes sumas de dinero en pequeñas transacciones para evitar los sistemas de detección de lavado de dinero. Esto hacía más difícil para las autoridades detectar un patrón claro de actividades ilícitas.

d. Casos de lavado de activos mediante el uso de Bitcoin ATM

i. *EEUU (año 2019)*

En 2019, en Los Ángeles, un operador de una red de Bitcoin ATM fue arrestado y acusado de lavado de dinero por facilitar el intercambio de grandes cantidades de efectivo de origen ilícito en Bitcoin.

En este caso, el imputado permitía a los usuarios convertir efectivo en Bitcoin sin registrar la identidad de los clientes, a pesar de que la ley exigía que lo hiciera.

De esta manera, los delincuentes depositaban grandes cantidades de dinero en efectivo en las máquinas, convirtiéndolas en criptomonedas que luego podían transferir de manera anónima, dificultando el rastreo del origen ilícito de los fondos.

ii. *España (año 2020)*

En 2020, la Guardia Civil española desmanteló una organización criminal que utilizaba Bitcoin ATM (BTM) para lavar dinero proveniente del tráfico de drogas. Los narcotraficantes usaban estos cajeros automáticos de criptomonedas para blanquear

grandes cantidades de dinero en efectivo -derivadas de la venta de drogas en el mercado negro-, dado que estos dispositivos no siempre requieren los estrictos procesos de verificación que las instituciones bancarias tradicionales sí aplican.

Además, los delincuentes usaban técnicas de «smurfing» para dividir grandes sumas de dinero en montos pequeños, evitando los sistemas de alerta que se activan con transacciones de grandes cantidades -en concreto, hacían numerosos depósitos en cajeros Bitcoin en diferentes localidades para así disimular el origen de los fondos-.

Una vez convertidos en criptomonedas, los activos eran transferidos a varias billeteras digitales y «mixers» para ocultar el origen del dinero y romper cualquier vínculo con las actividades ilícitas. Luego, los fondos se movían a través de exchangers de criptomonedas, algunos de los cuales estaban ubicados en jurisdicciones con poca regulación o cooperación internacional.

Desafíos principales para las autoridades.

- *Falta de regulación clara*. En algunos países, la regulación de los Bitcoin ATM era ambigua, lo que dificultaba a las autoridades rastrear las transacciones o exigir un control de identidad riguroso en los depósitos y retiros.
- *Anonimato*. Los criminales aprovechaban la relativa facilidad con la que podían usar los BTM para hacer transacciones sin un nivel significativo de verificación de identidad.
- *Fragmentación de fondos*. Al dividir las transacciones en montos pequeños y realizar múltiples operaciones en diferentes cajeros, los criminales evitaban los umbrales que activan las alertas de posibles actividades de lavado de dinero.

5. Principales retos que implica el uso de criptomonedas en materia de lavado de activos a nivel investigativo

La irrupción de los activos virtuales -entre los cuales indudablemente se encuentran las criptomonedas- en el mundo criminal, concretamente como elementos para desarrollar nuevas modalidades de lavado de activos, impone adaptar las investigaciones a las características propias del ciberespacio, un escenario completamente diferente de aquél en que tradicionalmente se desarrolla esta particular tipología criminal.

Para las agencias encargadas de perseguir el lavado de activos ello supone nuevos obstáculos y desafíos que, a su vez, demandan nuevas estrategias y metodologías para asegurar la eficacia de su investigación.

Sobre este punto, el GAFILAT (2021: 41) sostiene que:

> En cuanto atañe a los obstáculos y desafíos, sobresalen el carácter 'extraterritorial' atribuido al ciberespacio por muchos expertos; la libertad y velocidad del intercambio de datos informáticos (incluyendo los que pueden ser relevantes como evidencia o para identificar AV susceptibles de incautación o decomiso) a través de la Internet; el fenómeno de la 'pérdida de conocimiento de la localización' de esos datos y la consecuente dificultad para establecer la ley procesal que debe regir su recolección. A ello viene a sumarse la aparición de novedosas tecnologías que impiden -o cuanto menos dificultan en gran medida- el ejercicio, por parte de las agencias policíacas, de las facultades de vigilancia que las leyes locales les confieren,

> entre las que cabe mencionar -además de las relacionadas al funcionamiento de los AV- a los nuevos métodos de comunicación que sustituyen a la Red Telefónica Pública Conmutada (RTPC), los sistemas de navegación anónima en la Internet y la encriptación de comunicaciones y contenidos almacenadas, entre otros.

Los casos analizados en el capítulo anterior exponen, con matices diferenciados, las implicancias del uso de criptomonedas con fines ilícitos, específicamente en torno al lavado de activos, dejando además en evidencia algunos de los principales retos que supone para las agencias encargadas de su persecución.

a. Pseudoanonimato. Anonimato parcial. Anonimato total. Transacciones confidenciales.

Para comenzar, hemos de referir que, en lo que respecta a la identidad de los usuarios asociados con las direcciones involucradas, la blockchain no proporciona ningún dato personal -como ser nombres, domicilios, abonados telefónicos, correos electrónicos-, dado que no es necesario brindar esa información para realizar las operaciones y el protocolo que determina su funcionamiento no prevé siquiera la inserción de esos datos en la cadena de bloques.

Asimismo, tampoco se almacenan las direcciones IP utilizadas para realizar las transferencias entre las partes. De hecho, aunque los nodos que participan en la red podrían determinar desde qué IP se origina una transacción, debido a la forma en que se distribuyen y retransmiten las operaciones en la red -donde no hay una entidad central que controle todas las transacciones, sino que son los propios nodos quienes las validan y transmiten-, resulta extremadamente complicado identificar de manera precisa qué nodo en particular inició una determinada operación.

A pesar de ello, no es del todo correcto afirmar que las transacciones con criptoactivos son completamente anónimas. En rigor de verdad, debido a sus características, es necesario utilizar métodos adicionales, más allá del simple análisis de la base de datos, para identificar a las personas detrás de cada dirección.

En este orden de cosas, el Grupo de Acción Financiera de Latinoamérica -GAFILAT- (2021: 41 y ss.) sostiene que:

> […] las distintas criptomonedas implementan una serie de desarrollos tecnológicos adicionales dirigidos a incrementar el anonimato de los/las usuarios. Así, de acuerdo al modo en que están estructuradas, estos activos virtuales pueden ofrecer cuatro niveles distintos de anonimato, a saber: 1) pseudo anonimato: derivado del uso de pseudónimos (direcciones alfanuméricas) para oscurecer la identidad del/la usuario/a; 2) anonimato parcial («set anonymity»), en el que la identidad del/la verdadero/a usuario/a puede ser una entre varias posibles, lo que se consigue mediante el uso de 'firmas en círculo'; 3) anonimato total del/la usuario/a, la cual se obtiene cuando el/la verdadero/a puede ser cualquiera de los nodos del sistema; y 4) transacciones confidenciales, en las que se garantiza que los montos transferidos también permanecen ocultos.

b. Falta de regulación global

En el plano estrictamente legal, siendo que las criptomonedas operan en una red global, no existe a su respecto una regulación uniforme, toda vez que algunos países tienen marcos legales rigurosos, mientras que en otros la regulación es laxa o inexistente,

lo que permite a los delincuentes trasladar fondos a través de jurisdicciones con baja supervisión para asegurar así el producto de sus fechorías.

Explica al respecto Adra (2021):

> Si tenemos que hablar del derecho internacional, podemos decir que no hay una regulación específica en cuanto a la comisión de delitos por el uso de criptomonedas, sino que más bien hay una guía de recomendaciones establecidas por el GAFI -a través de las llamadas FATF Recommendations- o por la 'Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional'[…]

c. Descentralización

Tampoco existe en relación a las criptomonedas una autoridad central que controle el flujo de los activos virtuales. Las criptomonedas, al estar descentralizadas, permiten a los individuos tener control total sobre sus activos, pudiendo realizar transacciones directamente entre ellos sin necesidad de intermediarios.

d. Localización

A su vez, su localización puede ser fija como no serlo; entran a jugar aquí los llamados monederos, que consisten en un medio físico, un dispositivo, un programa o un servicio utilizado por los poseedores de criptomonedas para almacenar (múltiples) claves públicas y/o privadas, necesarias para realizar todo tipo de transacciones.

Los monederos se usan para rastrear la propiedad y para recibir y gastar criptomonedas. Ahora bien, cuando se trata de monederos *online*, la información suele estar almacenada en servidores ubicados en *data centers* localizados en puntos estratégicos del globo. Además, los datos pueden estar en un solo lugar o distribuidos en varios servidores de diferentes países y reacomodarse automáticamente, o almacenados en forma redundante en múltiples copias para ser recuperados si falla un servidor.

Ello hace que, en ocasiones, ni la propia compañía que brinda el servicio de almacenamiento en la nube pueda establecer dónde se encuentra un conjunto específico de datos digitales -como puede ser un monedero Bitcoin- en un momento determinado; y que tampoco las autoridades interesadas en la investigación de dicha información, por su posible conexión con algún delito en particular, tengan acceso a ese dato.

Lo expuesto implica que, incluso frente a la necesidad de concretar la incautación o el decomiso de las criptomonedas, no se sepa con exactitud qué país tiene jurisdicción para disponer la medida cautelar.

A esta problemática en particular alude Spoenle (2010), refiriéndose a la misma como «loss of location». El autor apuntado explica que los datos en la nube se transfieren constantemente de un servidor a otro, moviéndose dentro o a través de diferentes países en cualquier momento. Sostiene que estos datos podrían reflejarse -*mirroring*- por razones de seguridad y disponibilidad y, por lo tanto, encontrarse en forma simultánea en múltiples ubicaciones dentro de un país o en varios países separados. Debido a esto, puede suceder que ni siquiera el proveedor de computación en la nube sepa dónde se ubican exactamente los datos.

Concluye su razonamiento afirmando que la ubicación, como variable constante aplicable a todos los objetos tangibles y a objetos de datos intangibles desde que Internet

también se hizo popular, ha dejado de funcionar bajo las condiciones de la computación en la nube -*cloud computing*-.

e. Tecnologías de «anonimato por diseño»

La aparición de herramientas tecnológicas que debilitan el anonimato ofrecido por Bitcoin y otras criptomonedas tradicionales ha derivado en la creación de nuevas alternativas, conocidas como *privacy coins* -monedas privadas-, que a través de la implementación de diversos mecanismos aseguran un mayor nivel de anonimato a sus usuarios. Para ejemplificar la cuestión, haremos hincapié en dos de las principales *privacy coins* que existen a la fecha, Monero y Zcash.

Monero (XMR) - a diferencia de las alternativas selectivamente transparentes, Monero es la única criptomoneda en la que cada usuario es anónimo por defecto. El remitente, el receptor y el importe de cada transacción se ocultan mediante el uso de tres importantes tecnologías: direcciones secretas, firmas de anillo y RingCT.

- *Direcciones secretas (stealth adresses)*. Las direcciones ocultas son una parte importante de la privacidad inherente de Monero. Permiten y requieren que el remitente cree direcciones únicas aleatorias para cada transacción en nombre del destinatario. El destinatario puede publicar solo una dirección, pero todos sus pagos entrantes van a direcciones únicas en la cadena de bloques, donde no pueden vincularse ni a la dirección publicada del destinatario ni a ninguna otra dirección de transacción. Al utilizar direcciones ocultas, sólo el remitente y el destinatario pueden determinar dónde se envió el pago.

En otras palabras, cada vez que alguien envía Monero, se genera una dirección única y aleatoria para esa transacción, conocida como «dirección furtiva». Esto significa que, aunque una transacción sea visible en la blockchain, no se puede vincular directamente al receptor, ya que la dirección del receptor real no se muestra públicamente.

- *Firmas de anillo (ring signatures)*. En criptografía, una firma en anillo es un tipo de firma digital que puede realizar cualquier miembro de un grupo de usuarios, cada uno de los cuales tiene claves. Por lo tanto, un mensaje firmado con una firma en anillo está respaldado por alguien de un grupo particular de personas. Una de las propiedades de seguridad de una firma en anillo es que debería ser computacionalmente inviable determinar cuál de las claves de los miembros del grupo se utilizó para producir la firma.

Por ejemplo, se podría utilizar un anillo de firma para proporcionar una firma anónima de «un funcionario de alto rango de la Casa Blanca», sin revelar qué funcionario firmó el mensaje. Las firmas en anillo son adecuadas para esta aplicación porque el anonimato de una firma en anillo no se puede revocar y porque el grupo para una firma en anillo se puede improvisar (no requiere configuración previa).

En el caso de Monero, una firma en anillo utiliza las claves de su cuenta y una serie de claves públicas (también conocidas como salidas) extraídas de la cadena de bloques mediante un método de distribución triangular. Con el paso del tiempo, los resultados anteriores podrían utilizarse varias veces para formar posibles participantes firmantes. En un «*anillo*» de posibles firmantes, todos los miembros del anillo son iguales y válidos. No hay forma de que un observador externo pueda saber cuál de los posibles firmantes de un grupo de firmas pertenece a su cuenta. Por lo tanto, las firmas en anillo garantizan

que los resultados de las transacciones no sean rastreables. Además, no hay problemas de fungibilidad con Monero dado que cada resultado de transacción tiene una negación plausible (por ejemplo, la red no puede decir qué resultados se gastan y qué no se gastan).

En términos menos complejos, esta tecnología combina las entradas de una transacción con otras entradas aleatorias en la red, de manera que es casi imposible identificar qué entrada es la real. Esto oculta al remitente de la transacción al difuminar su participación entre varias posibles entradas.

- *Ringct (ring condifential transactions).* Es una versión mejorada de las firmas de anillo llamada «una firma de grupo anónimo espontáneo vinculable de múltiples capas», que permite ocultar cantidades, orígenes y destinos de las transacciones de forma tal que se mantienen confidenciales mientras siguen siendo verificables por los nodos de la red.
- *Zcash (zec).* Es una criptomoneda similar a Bitcoin en su diseño (de hecho, se creó a partir del código base original de Bitcoin), pero utiliza una tecnología de privacidad que cifra la información de las transacciones y permite a los usuarios proteger sus activos.

Al igual que Monero, tiene un fuerte enfoque en la privacidad, pero permite a los usuarios elegir entre realizar transacciones públicas o privadas, ofreciendo más flexibilidad.

Utiliza una tecnología innovadora llamada zk-SNARK (Zero Knowledg-Succinct Non-Interactive Argument of Knowledge), que permite validar transacciones sin revelar detalles como las direcciones de los remitentes y receptores, o los montos involucrados.

Las pruebas de «conocimiento cero» permiten a una parte (el probador) demostrarle a otra (el verificador) que una afirmación es verdadera, sin revelar ninguna información más allá de la validez de la afirmación misma. Por ejemplo, dado el hash de un número aleatorio, el probador podría convencer al verificador de que efectivamente existe un número con este valor hash, sin revelar cuál es.

En una «prueba de conocimiento» de conocimiento cero, el demostrador puede convencer al verificador no sólo de que el número existe, sino de que, de hecho, conoce ese número, nuevamente, sin revelar ninguna información sobre el número.

A su vez, Zcash ofrece la posibilidad de llevar adelante transacciones de dos tipos: transparent y shielded (transparentes y blindadas). Si bien la mayoría de las cadenas de bloques exponen públicamente toda la información de transacciones y saldos, con Zcash existe la opción de mantener la información financiera privada (shielded) o transparente y disponible para el público como la mayoría de las otras cadenas de bloques.

He aquí una diferencia fundamental con Monero, dado que ésta oculta de forma predeterminada toda la información de las transacciones, ofreciendo privacidad total por defecto, mientras que Zcash permite elegir entre transacciones públicas y privadas, utilizando zk-SNARKs para las transacciones blindadas.

f. Plataformas de intercambio descentralizadas (DEXs)

Los DEXs son plataformas que permiten el intercambio de criptomonedas y tokens de manera descentralizada, esto es, sin la necesidad de un intermediario. A diferencia de los exchanges centralizados (CEX), donde un bróker controla los fondos y transacciones, en un DEX los usuarios tienen control total de sus activos gracias a los contratos inteligentes, que ejecutan y verifican transacciones en un entorno completamente transparente.

Este tipo de plataformas habilitan los intercambios directos P2P entre usuarios/as de criptomonedas y explotan innovaciones tecnológicas como las cuentas de fondos en custodia *-e-scrow accounts-* multi-firma para permitir que los/las usuarias intercambien activos virtuales sin necesidad de un tercero que custodie los fondos.

6. Marco regulatorio cripto

a. El panorama internacional.

La adopción de los activos virtuales -como medios de inversión, ahorro, para realizar transacciones, etc.- se presenta como una tendencia creciente a nivel global. En este sentido, dentro del índice general de adopción cripto para el año 2022 publicado por Chainalysis, cinco países miembros del GAFILAT -Brasil (7°), Argentina (13°), Colombia (15°), Ecuador (18°) y Méjico (28°)- aparecen posicionados entre los primeros 30 lugares, lo que refuerza la necesidad de emitir una regulación adecuada que cumpla con los estándares del GAFI, proporcione certeza a quienes operan con este tipo de activos dentro de la región del GAFILAT, y aborde los riesgos a los que se encuentran expuestos los diferentes actores.

En relación a la temática que nos compete en este punto, Adra (2021) afirma:

> Podemos clasificar en tres grupos las respuestas dadas por los países para combatir el lavado. El primer grupo lo integran los que han optado por la inacción, que son la mayoría de los países. Esto se debe a que no han elaborado ningún tipo de normativa regulando las criptomonedas, por la dificultad que implica el desafío de entender cabalmente todas las aristas de esta novedosa teconología...En el segundo grupo, podemos encontrar la postura que se encontraría en el otro extremo, que es la prohibición del uso de criptomonedas...Por último, se encuentran los países que optaron por la regulación. Este es el grupo más complejo, en el que cada país tiene sus matices propios con respecto a la normativa aplicable.

A nivel internacional, no existe una regulación específica o integral respecto al uso de activos virtuales para la comisión de lavado de dinero; en su lugar, aparecen las Recomendaciones del GAFI, definidas como «un esquema de medidas completo y consistente que los países deben implementar para combatir el lavado de activos […]» -GAFI, 2020), que fijan un estándar internacional que los Estados han de poner en práctica mediante la adopción de medidas ajustadas a sus circunstancias particulares, ello teniendo en cuenta la existencia de diversos marcos legales, administrativos y operacionales, y diferentes sistemas financieros.

En este sentido, según expresa Biagosch. (2018: 399):

> de acuerdo con el Grupo Internacional de Acción Financiera, la correcta aplicación de las recomendaciones sobre PLA/FT posibilita que los países puedan: I) proteger las instituciones públicas; II) aumentar la transparencia del sistema financiero; y III) facilitar la detección, investigación y enjuiciamiento del delito de lavado de activos y sus delitos precedentes, así como el recupero de los fondos sustraídos.

Entre las medidas consideradas esenciales por parte del GAFI se encuentran las siguientes:

- identificar los riesgos, y desarrollar políticas y coordinación internas;
- luchar contra el lavado de activos; financiamiento del terrorismo y financiamiento de la proliferación;
- aplicar medidas preventivas para el sector financiero y otros sectores designados;
- establecer poderes y responsabilidades (por ejemplo, autoridades investigativas, de orden público y de supervisión) y otras medidas institucionales;
- mejorar la transparencia y la disponibilidad de la información de sobre el beneficiario final de las personas y estructuras jurídicas; y
- facilitar la cooperación internacional.

Como no pretendemos aquí realizar un análisis pormenorizado del catálogo de recomendaciones del GAFI, haremos una breve reseña de las que, entendemos, se vinculan con el tópico de esta investigación.

Así entonces, la Recomendación 1 establece que los países deben identificar, evaluar y entender sus riesgos de lavado de activos/financiamiento del terrorismo, y deben tomar acción y aplicar recursos encaminados a asegurar que se mitiguen eficazmente los riesgos. Además, aplicar un enfoque basado en riesgo (EBR) para asegurar que las medidas adoptadas en pos de prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados.

La Recomendación 2 establece la necesidad de cooperación y coordinación nacional, aclarando que los países deben contar con políticas ALA/CFT/CFP a escala nacional, que tomen en cuenta los riesgos identificados, las cuales deben ser sometidas a revisión periódicamente, y deben designar a una autoridad o contar con un mecanismo de coordinación o de otro tipo que sea responsable de dichas políticas.

La Recomendación 3 propone tipificar el lavado de activos en base a la Convención de Viena y la Convención de Palermo, agregando que deben aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor gama posible de delitos determinantes.

La Recomendación 4 sugiere la adopción de medidas similares a las establecidas en la Convención de Viena, la Convención de Palermo y el Convenio Internacional para la Represión de la Financiación del Terrorismo, que permitan a sus autoridades congelar o incautar y decomisar bienes y/o productos relaciones con el lavado de dinero.

La Recomendación 9 exhorta a asegurar que las leyes sobre el secreto de la institución financiera no impidan la implementación de las Recomendaciones del GAFI.

La Recomendación 10 se refiere a la debida diligencia del cliente, y comienza con la prohibición a las instituciones financieras de mantener cuentas anónimas o cuentas con nombres ficticios

Dispone, a su vez, la necesidad de exigir a las instituciones financieras que emprendan medidas de Debida Diligencia del Cliente (DDC) cuando: (i) establecen relaciones comerciales; (ii) realizan transacciones ocasionales: (i) por encima del umbral aplicable designado (USD/EUR 15,000); o (ii) están ante transferencias electrónicas en las circunstancias que aborda la Nota Interpretativa de la Recomendación 16; (iii) existe una sospecha de lavado de activos o financiamiento del terrorismo; o (iv) la institución financiera tiene dudas sobre la veracidad o idoneidad de los datos de identificación sobre el cliente obtenidos previamente.

A su vez, entre las medidas de DDC a adoptarse, se proponen:

> (a) Identificar al cliente y verificar la identidad del cliente utilizando documentos, datos o información confiable, de fuentes independientes. (b) Identificar al beneficiario final y tomar medidas razonables para verificar la identidad del beneficiario final, de manera tal que la institución financiera esté convencida de que conoce quién es el beneficiario final. Para las personas jurídicas y otras estructuras jurídicas, esto debe incluir que las instituciones financieras entiendan la estructura de titularidad y de control del cliente. (c) Entender, y cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial. (d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

La Recomendación 11 exige que las instituciones financieras mantengan registro de sus operaciones por espacio de al menos cinco años, ello ante posibles pedidos de información por parte de las autoridades competentes.

La Recomendación 15 demanda de los países e instituciones financieras la identificación y evaluación de los riesgos de lavado de activos que pudieran surgir con respecto al desarrollo de nuevos productos y prácticas comerciales, o a partir de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes.

La Recomendación 18 exige a las instituciones financieras la implementación de programas contra el lavado de activos, incluyendo políticas y procedimientos para intercambiar información dentro del grupo para propósitos ALA/CFT.

Las Recomendaciones 24 y 25 sostienen que los países tienen que implementar medidas para impedir el uso indebido de personas jurídicas u otras estructuras jurídicas con fines de lavado de activos.

La Recomendación 26 establece la necesidad de que las instituciones financieras estén sujetas a una regulación y supervisión adecuadas y que implementen eficazmente las Recomendaciones del GAFI.

La Recomendación 28 se refiere a las Actividades y Profesiones No Financieras Designadas, las que deben quedar sujetas a sistemas eficaces para el monitoreo y aseguramiento del cumplimiento de las normas ALA -anti lavado activos-.

La Recomendación 37 trata de la asistencia legal mutua, puntualizando en la necesidad de que los países presten rápida, constructiva y eficazmente, el mayor rango posible de asistencia legal mutua con relación a investigaciones, procedimientos judiciales y procesos relacionados con el lavado de activos.

La Recomendación 38 complementa la anterior, ordenando a los países tomen acción rápida en respuesta a solicitudes extranjeras para identificar, congelar, embargar y

decomisar bienes lavados; productos del lavado de activos y de los delitos determinantes; instrumentos utilizados en, o destinados para ser usados en, la comisión de estos delitos; o bienes de valor equivalente.

La Recomendación 39 sostiene que los países deben ejecutar constructiva y eficazmente, las solicitudes de extradición con relación al lavado de activos.

Finalmente, la Recomendación 40 insta a que los países, a través de sus autoridades, presten el mayor rango de cooperación internacional con relación al lavado de activos y delitos determinantes asociados.

b. El caso de argentina

En nuestro país no existe un marco legal unificado sino diversas regulaciones enfocadas en aspectos relacionados con la operación de los Proveedores de Servicios de Activos Virtuales -PSAV- y con los Activos Virtuales -AV- propiamente dichos.

En materia de lavado de activos, el antecedente legal más destacado lo encontramos en la sanción de la Ley 25.246 (B.O. 10/5/2000), mediante la cual se reformó el Código Penal para tipificar los delitos de LA, se creó la Unidad de Información Financiera (UIF) -organismo autónomo y autárquico que funciona bajo la órbita del Ministerio de Justicia y se encarga del análisis, el tratamiento y la transmisión de información a los efectos de prevenir e impedir el Lavado de Activos (LA), la Financiación del Terrorismo (FT) y el Financiamiento de la Proliferación de armas de destrucción masiva (FP)- y se establecieron las acciones ALA/CFT, particularmente la identificación de los sujetos obligados a informar a la UIF, las acciones de «debida diligencia» (DDC) que deben llevar adelante en materia de «conocimiento del cliente» y de información, análisis y presentación de reportes de operaciones sospechosas (ROS).

Esta norma fue modificada sustancialmente por la ley 26.683 (B.O. 21/6/2011), que produjo una reestructuración integral del delito de lavado de activos de origen ilícito al dejar de regularlo como una de las categorías propias del encubrimiento y establecerlo como un delito autónomo.

Encontramos también la ley 27.430, que modificó el sistema tributario argentino para incluir en el imputado a las ganancias los resultados obtenidos por la enajenación de monedas digitales.

Más recientemente, en lo que considero un avance importante en la materia, se sancionó la ley 27.739 (B.O. 15/3/24), mediante la cual se reformó el *sistema normativo nacional de prevención en lavado de activos y financiación del terrorismo* (LA/FT) y se crearon las definiciones básicas para la regulación y supervisión de los activos digitales o criptoactivos junto con la actividad de sus operadores.

Los ejes principales de la norma incluyen modificaciones al código penal -arts. 41 quinquies, 303 y 306-, a la Ley 25.246 y sus modificatorias -incorporación de los arts. 4 bis, 17 bis, 24 bis, 27 bis, sustitución de los arts. 5, 13, 14, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, modificación del inc. g) del art. 9°, incorporación del capítulo VI, derogación de los arts. 20 bis y 21 bis-, la creación de un registro de activos virtuales (tal como dicho término se define más abajo) y la definición de la figura de los proveedores de servicios de activos virtuales -PSAV-.

A su vez, amplió el catálogo de operaciones que se deben informar a la UIF y dispuso la incorporación de los PSAV, a las personas humanas o jurídicas que realizan, en nombre

de un tercero, custodia y administración de efectivo o valores líquidos, abogados y proveedores de servicios societarios y fiduciarios.

Definió los activos virtuales como una «representación digital de valor que se puede comercializar y/o transferir digitalmente y utilizar para pagos o inversiones».

Creó también el Registro de Proveedores de Servicios de Activos Virtuales, disponiendo que estará a cargo de la Comisión Nacional de Valores -CNV-, ello con el objetivo de centralizar la información sobre individuos y empresas que ofrecen servicios relacionados con Activos Virtuales; y también el Registro Público de Beneficiarios Finales, a cargo de la AFIP, encargado de centralizar información adecuada, precisa y actualizada de aquellas personas humanas que revisten el carácter de beneficiarios finales en los términos definidos en el art. 4° bis de la Ley N° 25.246.

Por otro lado, en lo que respecta a la normativa de jerarquía inferior a las leyes, aparecen las resoluciones de la UIF, entre las cuales cobra especial relevancia la Resolución 300 del año 2014, que en su art. 1° establece que los Sujetos Obligados enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del artículo 20 de la Ley Nº 25.246 y sus modificatorias deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales y establecer un seguimiento reforzado respecto de estas operaciones, evaluando que se ajusten al perfil del cliente que las realiza, de conformidad con la política de conocimiento del cliente que hayan implementado.

Por su parte, la Resolución General 4614/2019 de la AFIP impone a los sujetos que administren servicios de procesamiento de pagos a través de plataformas de gestión electrónica o digital a cumplir con un régimen informativo mensual sobre sus transacciones, debiendo reportar monto total de los ingresos y egresos, tipo de ingreso (efectivo, transferencia, moneda digital, moneda extranjera), saldo mensual de las cuentas en moneda de curso legal, en moneda extranjera y/o en moneda digital o criptomoneda.

Finalmente, encontramos la Comunicación A 7759 del Banco Central de la República Argentina, que prohíbe a los Proveedores de Servicios de Pago que ofrecen Cuentas de Pago realizar o facilitar a sus clientes la realización de operaciones con activos digitales -incluidos los criptoactivos y aquellos cuyos rendimientos se determinen en función de las variaciones que esos registren- que no se encuentren autorizados por una autoridad reguladora nacional competente ni por el Banco Central de la República Argentina.

c. La situación en la UE

La idea de establecer un marco regulatorio en materia de criptomonedas en la U.E. comenzó alrededor del año 2017, con el auge del Bitcoin. Tanto es así que, al año siguiente, se aprobó la Quinta Directiva contra el Lavado de Dinero (5AMLD), que incluyó a los PSAV -Proveedor de Servicios de Activos Virtuales, o CASP por sus siglas en inglés- dentro del alcance de la legislación AML/CFT de la UE por primera vez.

Esto requirió que los PSAV cumplieran con las mismas reglas que las instituciones financieras tradicionales, incluida la identificación del cliente, la verificación de identidad, el monitoreo de transacciones y la notificación de transacciones sospechosas.

A pesar de esto, muchos proveedores de servicios y activos criptográficos aún no estaban dentro del alcance regulatorio, y estos puntos ciegos dejaban a los consumidores e inversores expuestos a un riesgo sustancial.

Además, algunos estados miembros de la U.E. implementaron sus propias reglas criptográficas, quedando fuera de la regulación actual de la U.E. y generándose una fragmentación regulatoria.

Como resultado, la Comisión Europea comenzó a delinear regulaciones de armonización (MiCA) que se aplicarían en toda la U.E., y finalizó el primer borrador en 2020. Desde entonces, MiCA se ha modificado y mejorado para cubrir todos los tipos de criptoactivos y los posibles problemas que puedan surgir.

El MiCA -Markets in Crypto-Assets por sus siglas en inglés- es el marco regulatorio europeo para los criptoactivos. Se trata de una legislación integral cuyo propósito es establecer reglas uniformes para los emisores de criptoactivos que hasta el momento no han sido regulados por otras normas de la U.E.

Esta legislación abarca una amplia gama de aspectos relacionados con los criptoactivos, como su definición, requisitos de licencia para los PSAV, adopción de normativas para la protección de los inversores y medidas para prevenir su uso para actividades ilícitas.

MiCA entró oficialmente en vigor el 9 de junio de 2023. A su vez, las disposiciones sobre tokens referenciados a activos y tokens de dinero electrónico comenzaron a regir a partir del 30 de junio de 2024, y tendrán aplicación plena desde el 30 de diciembre de 2024.

En definitiva, MiCA establece un marco integral para los criptoactivos en la UE, que abarca la emisión, oferta, negociación y custodia. También introduce requisitos de licencia para los PSAV, establece reglas para las stablecoins, prohíbe el abuso de mercado y refuerza la protección del consumidor.

Esto supone mayores márgenes de certeza para las empresas que trabajan con criptomonedas, creando un sistema unificado en toda la UE, y si bien es muy probable que las regulaciones se vuelvan más estrictas, esto minimizará los riesgos tanto para las empresas como para los clientes.

d. Brasil

En diciembre de 2022, Brasil publicó la Ley 14.478, que proporciona nuevas directrices para los proveedores de servicios de activos virtuales y define los delitos y el fraude utilizando activos virtuales.

En junio de 2023, el presidente Lula da Silva promulgó el decreto gubernamental No. 11.563, por el cual se autoriza al banco central a regular y supervisar a los proveedores de servicios de activos virtuales y garantiza que muchos proyectos simbólicos que califican como valores seguirán estando bajo la competencia de la comisión de bolsa y valores de Brasil.

En mayo de 2024, el Banco Central de Brasil anunció que las propuestas regulatorias para los criptoactivos estarían finalizadas a finales de año.

En el vecino país, si bien las criptomonedas no se reconocen como moneda de curso legal, se pueden poseer, comercializar y utilizar como medio de pago.

e. EEUU

En los Estados Unidos, las regulaciones en materia de criptoactivos varían según el estado. En general, la SEC solo regula las ventas de criptomonedas si 1) constituyen la venta de un valor según la ley estatal o federal, o 2) se consideran una transmisión de dinero según la ley estatal o una acción que convertiría a una persona en una empresa de servicios monetarios según la ley federal.

En lo que respecta a la evolución de ese marco regulatorio, en 2014, el Servicio de Impuestos Internos emitió directrices y esbozó principios generales sobre la tributación de las monedas virtuales.

En 2015, Nueva York se convirtió en el primer estado de EE.UU. en regular las criptomonedas. Desde entonces, muchos estados lo han seguido.

En 2016, la *comisión de comercio de futuros de productos básicos* (CFTC) ejerció por primera vez su poder para exigir que las bolsas de criptomonedas que ofrecen contratos de futuros se registren.

Al año siguiente, Estados Unidos reguló las ofertas iniciales de monedas, que estaban bajo la jurisdicción de la *comisión de bolsa y valores* (SEC), y la SEC publicó un informe en el que se destacaba que los tokens DAO son valores.

En 2018, el *servicio de impuestos internos* (IRS) actualizó las normas fiscales relativas a las transacciones de criptoactivos y estableció una fuerza fiscal sobre delitos fiscales transnacionales y lavado de dinero que cubría los criptoactivos.

El marco AML/CFT del país se actualizó en 2020 con modificaciones a la Ley contra el Lavado de Dinero.

Más recientemente, en 2022, el presidente Biden emitió una orden ejecutiva que ordena a varias agencias tomar medidas significativas para proteger a los consumidores, ampliar el acceso a los servicios financieros, garantizar la estabilidad financiera, combatir las finanzas ilícitas y más. Estados Unidos tiene un mercado de criptomonedas sustancial y ocupa el cuarto lugar en el índice de adopción global de criptomonedas de Chainalysis. El gobierno está considerando numerosos proyectos de ley sobre criptomonedas.

En julio de 2023, la *ley de certeza regulatoria de blockchain* fue aprobada por el comité de servicios financieros. El proyecto de ley «eximiría a ciertos desarrolladores y redes de blockchain de los requisitos de informes financieros y licencias requeridos por las leyes federales y estatales actuales».

Ese mismo mes, la *ley de claridad para las monedas estables de pago* tuvo aprobación por por el comité de servicios financieros de la cámara de representantes. El proyecto de ley serviría como el primer marco regulatorio federal integral sobre las monedas estables.

En igual fecha, la comisión de servicios financieros de la cámara de representantes aprobó la Ley Keep Your Coins. El proyecto de ley «prohibiría a las agencias federales restringir el uso de moneda virtual convertible por parte de una persona para comprar bienes o servicios para el propio uso de la persona y para otros fines».

El 29 de agosto de 2023, el IRS publicó una serie de normas propuestas que «requerirían que los corredores, incluidas las plataformas de comercio de activos digitales, los procesadores de pagos de activos digitales y ciertas billeteras alojadas en activos digitales, presenten declaraciones de información y proporcionen declaraciones de

beneficiarios sobre las disposiciones de activos digitales efectuadas para los clientes en ciertas transacciones de venta o intercambio».

En abril de 2024, se presentó en el senado la ley lummis-gillibrand de monedas estables de pago. Esta legislación propone un régimen regulatorio para las monedas estables, centrándose en la protección del consumidor, las normas AML/CFT y la preservación del dominio del dólar estadounidense.

En mayo de 2024 se aprobó la ley de innovación y tecnología financiera para el siglo XXI, que busca expandir el poder regulatorio de la CFTC, aclarar el papel de la SEC y definir cuándo una criptomoneda es un valor o una mercancía.

También en 2024, el IRS publicó un borrador de su nuevo formulario para informar los ingresos generados por las transacciones de activos digitales, que deberán completar los corredores de criptoactivos a partir de 2025.

En materia de AML/CFT, los intercambios de criptoactivos y los proveedores de servicios deben registrarse en FinCEN, cumplir con los requisitos AML/CFT y reportar cierta información a los reguladores.

f. China

Como contraste con los marcos regulatorios anteriormente descriptos encontramos la situación de China, donde las criptomonedas están virtualmente prohibidas.

El primer paso de China para regular los criptoactivos se produjo en 2013, cuando el Banco Popular de China prohibió a las instituciones financieras negociar con Bitcoin u otros activos virtuales.

En 2017, el gobierno chino prohibió también las ofertas iniciales de monedas y que las bolsas de criptoactivos operaran en China; esto último obligó a muchas bolsas que tenían su sede en China -incluida Binance, la más grande del mundo- a reubicarse.

Más recientemente, en 2021, el gobierno chino prohibió la minería, ilegalizó las transacciones de criptomonedas y bloqueó a las bolsas de criptomonedas extranjeras para que ofrecieran servicios a los ciudadanos chinos.

Sin embargo, si bien estas regulaciones prohíben efectivamente las criptomonedas en China, técnicamente a los ciudadanos chinos se les permite poseer criptoactivos, a punto tal que Chainalysis ubica a China en el puesto 11 a nivel mundial en adopción de criptomonedas.

7. Conclusiones

El auge de las criptomonedas ha revolucionado el panorama financiero mundial, pero también ha introducido nuevos desafíos en la lucha contra el lavado de activos. La naturaleza pseudónima y transfronteriza de las criptomonedas -por mencionar solo algunas de sus características- las convierte en un atractivo vehículo para actividades ilícitas.

El trabajo que nos convoca expone, con meridiana claridad, que la regulación de las criptomonedas representa un desafío complejo que busca, por un lado, prevenir actividades ilícitas como el lavado de activos y, por otro, fomentar la innovación y el uso

legítimo de estas tecnologías. Lograr este equilibrio es fundamental para garantizar la integridad del sistema financiero y, al mismo tiempo, promover el crecimiento económico.

Esta particular visión coincide con lo expuesto por Dellepiane, C. (2019), quien afirma que:

> […] Si pensamos en los diferentes objetos o mercancías que fueron utilizados como dinero a lo largo de la historia, la sal, la cebada y luego las primeras monedas acuñadas, el factor común que les posibilitó cumplir con su función ha sido la confianza, la ausencia de regulación puede ser causa de una posterior degradación de los instrumentos, a medida que se detecten casos de uso ilegitimo.

En tal sentido, se impone la obligación para el Estado de adecuar su legislación, acorde a un mapa de riesgos que permita la adopción de medidas oportunas, ágiles y proporcionales, para la detección de nuevos procedimientos e instrumentos y, acorde con ello, el dictado oportuno de nuevas regulaciones; todo ello, exige la integración de los reguladores con el trabajo de expertos del sector Fintech».

En este contexto, la comunidad internacional ha respondido con una serie de regulaciones diseñadas para prevenir y detectar el criptolavado. Normativas como la Regla de Viaje y los requisitos KYC/AML han sido implementadas en numerosos países, buscando aumentar la transparencia y trazabilidad de las transacciones.

Así entonces, frente al anonimato de las transacciones que va de la mano con la utilización de criptomonedas se deberían implementar medidas de «Conozca a su Cliente» (KYC, por sus siglas en inglés) y/regulaciones anti-lavado (o AML, por sus siglas en inglés), sin sacrificar por completo la privacidad. La tecnología blockchain, al ser un libro de contabilidad público, ofrece oportunidades para rastrear transacciones sin revelar la identidad de los usuarios en todos los casos.

Por otro lado, frente a un escenario global donde existen múltiples regulaciones en la materia se estima indispensable la armonización de tales normativas. En esta armonización juega un papel sumamente relevante el Grupo de Acción Financiera Internacional (GAFI), que ha permitido establecer estándares globales para la reglamentación de los activos virtuales, adoptados por la mayoría de los Estados modernos.

Además, toda vez que el uso de criptomonedas no aparece limitado por fronteras geográficas, la cooperación internacional es esencial, sobre todo cuando se utilizan para actividades ilícitas. Es allí donde el intercambio ágil de información entre los Estados y la coordinación de esfuerzos entre las agencias que aplican la ley y las entidades gubernamentales de diferentes países puede ayudar a prevenir, mitigar y/o sancionar a quienes actúan por fuera de la ley.

A nivel interno, en lugar de aplicar una regulación uniforme a todos los actores del mercado se pueden implementar enfoques basados en el riesgo, supervisando de manera más estricta a aquellos que presentan un mayor riesgo de actividades ilícitas.

Algunas de las herramientas de prevención de lavado de activos más eficaces vienen de la mano del licenciamiento de los PSAV -esto es, exigir a las plataformas de intercambio de criptomonedas y otros PSAV una licencia para supervisión y control de sus operaciones- y la adopción de la Travel Rule -una demanda del grupo GAFI para que los PSAV compartan información relevante sobre el originador y el beneficiario de las transacciones con activos virtuales-.

Sin embargo, la rápida evolución de la tecnología y la fragmentación regulatoria a nivel mundial presentan obstáculos significativos. A pesar de los avances, persisten desafíos importantes, como la proliferación de monedas estables y el desarrollo de protocolos de privacidad más sofisticados, que plantean nuevos retos para los reguladores. Además, la falta de coordinación entre diferentes jurisdicciones facilita que los delincuentes exploten las lagunas legales.

Es por ello que la investigación del delito de lavado de activos mediante el uso de criptomonedas demanda, por parte de los órganos encargados de la persecución penal, una exhaustiva capacitación en la materia que aborde no sólo el estudio de la tecnología de blockchain y las características de las criptomonedas, sino también el conocimiento de las regulaciones nacionales e internacionales en la materia y el proceso debido en materia de preservación e incorporación de evidencia digital al proceso.

En conclusión, el criptolavado representa un desafío complejo y en constante evolución. Si bien se han logrado avances significativos en la lucha contra este delito, es necesario un esfuerzo continuo por parte de los gobiernos, el sector privado y la sociedad civil para desarrollar soluciones innovadoras y efectivas. La clave para combatir el criptolavado radica en una combinación de regulación inteligente, tecnología avanzada y cooperación internacional.

8. Referencias

Adra, R. (2021). *Lavado de activos con criptomonedas: vulnerabilidades de control*. http://revele.uncoma.edu.ar/htdoc/revele/index.php/administracion

Biagosch, Z. A. (2018). La corrupción y la prevención del lavado de activos. En N. Durrieu & R. R. Saccani (Eds.), *Compliance, anticorrupción y responsabilidad penal empresaria* (p. 399). Thomson Reuters.

Botero Bernal, A. (2003). *La metodología documental en la investigación jurídica: alcances y perspectivas*. *Opinión Jurídica, 2*(4), 109–116. https://revistas.udem.edu.co/index.php/opinion/article/view/1350

Carrizo, R. (2003). *Tipificación del delito de lavado de activos de origen delictivo*. *LA LEY*, Sup.Act 08/07/2003.

Corbino, M. (2022). *El lavado de dinero a través de criptoactivos*. http://sedici.unlp.edu.ar/bitstream/handle/10915/137487/Documento_completo.pdf

De Marco, G. (2020). *Criptomonedas y ciberseguridad. Reflexiones sobre la situación regulatoria en el país, con motivo de una reciente decisión del Tribunal Superior de Nueva Zelanda*. *LA LEY*, SJA (15/05/2020), 7.

Dellepiane, C. L. (2019). *Los activos digitales como instrumento del lavado de dinero y financiamiento del terrorismo. Respuestas obligadas desde el compliance y la cooperación internacional*. *Revista de Derecho Empresario*, 1.

Donna, S. A. (2021). *Blockchain, criptomonedas y delito*. *Revista de Derecho Penal Económico: COVID y sus consecuencias jurídico-económicas*, 2021(2). Rubinzal-Culzoni.

Eraso Lomaquiz, S. E. (2015). *Las monedas virtuales en el Derecho argentino. Los Bitcoins*. *LA LEY* 31/12/2015, 1; *LA LEY 2016-A*, 727.

Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Europol Spotlight Report Series. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

Faliero, J. C. (2017). *E-lavado de activos: aristas y perspectivas*. *LA LEY*, SJA (31/05/2017), 8.

FATF–GAFI. (2015). *Guidance for a risk-based approach. Virtual currencies*.

Finol de Navarro, T., & Nava de Villalobos, H. (1996). *Procesos y productos en la investigación documental* (2.ª ed.). Universidad del Zulia.

Flores Dapkevicius, R. (2022). *Prevención de blanqueo de capitales con criptomonedas y non fungible tokens (NFTs). Cuál debida diligencia deben realizar los sujetos obligados*. https://cijur.mpba.gov.ar/files/bulletins/Rubén_Flores_Dapkevicius_V2_12-8.pdf

GAFI. (2014). *Monedas virtuales: definiciones claves y riesgos potenciales de LA/FT*.

GAFI. (2015). *Directrices para un enfoque basado en riesgo: monedas virtuales*. https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf

GAFI. (2020). *Recomendaciones del GAFI 2012: Actualizadas a octubre de 2020*. https://www.cfatf-gafic.org/es/documentos/recursos-del-gafic/14971-recomendaciones-del-gafi-2012-actualizadas-a-octubre-de-2020-1

GAFILAT. (2021). *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*. https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guía-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigación-identificación-incautación-y-decomiso-de-AV.pdf

Gómez Iniesta, D. (1996). *El delito de blanqueo de capitales en Derecho español*. Cedecs Editorial.

González Rossi, A. (2024). *Sobre el Registro de Proveedores de criptoactivos en la Argentina*. *LA LEY*, 29/04/2024, 1; *LA LEY 2024-B*, 316; *Enfoques 2024 (julio)*, 95.

Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*.

Lara Lara, J. A., & Muñoz Agudelo, M. A. (2017). *Análisis de los principales elementos del Bitcoin como criptomoneda y producto commodity en el comercio nacional*. Universidad La Salle.

Linares, M. B. (2019). Bitcoins: su empleo como técnica para lavar activos ilícitos. En *Temas de Derecho Penal y Procesal Penal* (p. 243 y ss.).

Linares, M. B. (2019). *Criptomonedas y lavado de activos*. *LA LEY*, DPyC (febrero), 213.

Marengo, F. (2011). *Aspectos generales del lavado de activos. El lavado de activos y la financiación del terrorismo. La problemática en el mercado de capitales*. https://www.pensamientopenal.com.ar/doctrina/28927-aspectos-generales-del-lavado-activos-lavado-activos-y-financiacion-del-terrorismo

Martínez, D. M. (2021). *Criptoactivos: ¿Nueva modalidad de lavado de activos?* https://www.pensamientopenal.com.ar/doctrina/89437-criptoactivos-nueva-modaldidad-lavado-activos

Mora, S. J. (2015). *Monedas virtuales: Una primera aproximación al Bitcoin*. *LA LEY*, 31/12/2015, 1.

MPF. (2023). *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos: Consideraciones teórico-prácticas sobre activos virtuales basados en blockchain y su investigación penal*. https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

Navarro Cardoso, F. (2019). *Criptomonedas (en especial, bitcóin) y blanqueo de dinero*. http://criminet.ugr.es/recpc/21/recpc21-14.pdf

Oppel, S. (2022). *Bitcoin: herramientas de análisis para abordar investigaciones penales que incluyan operaciones con esta cripto-moneda. Lineamientos para planificar una actividad cautelar eficiente*. *LA LEY*, DPyC (julio), 75.

Ortíz, J. C. (2020). *Lavado de activos: las monedas virtuales como herramienta del lavado. ¿Su utilización contradice las recomendaciones del GAFI? LA LEY*, DPyC (junio), 37.

Pérez López, X. (2017). *Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y España*. *Revista de Derecho Penal y Criminología*, 18, 141–187. https://core.ac.uk/download/475135308.pdf

Portillo, V. H. (2018). *El delito de ciberlavado de activos*. *LA LEY*, SJA 06/06/2018, 48.

Ruiz Gordillo, F. M. (2021). *La Ley Fintech como medio de prevención del lavado de dinero por parte de las instituciones de tecnología financiera*. *LA LEY*, DPyC (julio), 121.

Sánchez, O. (2017). *Bitcoin: Qué son las criptomonedas y cómo ganar dinero fácil con ellas*. San Bernardino, California.

Silvera Méndez, C. (2019). *Los desafíos ante la presencia de nuevos bienes jurídicos con especial atención en las criptomonedas*. *LA LEY*, DPyC 2020 (febrero), 196.

Skalany, E. G. (2019). *Criptomonedas y Derecho Penal en Argentina: Introducción a la blockchain, el bitcoin y más allá*. En *Enfoques actuales en los delitos contra el patrimonio*. Rubinzal-Culzoni.

Small, S. (2015). Bitcoin: The Napster or currency. *Houston Journal of International Law, 37*, 581.

Spoele, J. (2010). *Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df

Suárez Puga, E. A. (2021). *Naturaleza y régimen jurídico de las criptomonedas*. https://www.pensamientopenal.com.ar/doctrina/89427-naturaleza-y-regimen-juridico-criptomonedas

Unidad de Información Financiera. (2014). *Resolución UIF 300/2014*. https://www.argentina.gob.ar/normativa/nacional/resolución-300-2014-231930

Valdés Trapote, A. (2022). *Estudio sobre la lucha contra el lavado de activos mediante criptoactivos*. https://www.elpaccto.eu/wp-content/uploads/2022/07/Estudio-Lavado-Criptoactivos.pdf

Zoccaro, M. (2020). *El marco regulatorio de las criptomonedas en Argentina*. https://www.economicas.uba.ar/wp-content/uploads/2020/07/El-marco-regulatorio-de-las-criptomonedas-en-Argentina.pdf