EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Guía de investigación en el lavado de activos mediante criptodivisas

Ángel Bodoque Agredano

Alberto Orduna Lanau

Ediciones EL PAcCTO
Colección Herramientas

GUÍA DE INVESTIGACIÓN EN EL LAVADO DE ACTIVOS MEDIANTE CRIPTODIVISAS

Autores:

Ángel Bodoque Agredano
Alberto Orduna Lanau

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Edita: Programa EL PAcCTO
Calle Almansa 105
28040 Madrid (España)
www.elpaccto.eu

Bajo la coordinación de:

FIIAPP

EXPERTISE FRANCE

ALBERTO ORDUNA LANAU

Actualmente es Capitán del Grupo de Ciberinteligencia Criminal de la Unidad Técnica de Policía Judicial de la Guardia Civil. Master en Cómputo Forense e Investigación del Cibercrimen por el University College of Dublin, en sus más de treinta años de carrera profesional vinculados con la investigación e inteligencia tecnológica, ha ejercido, entre otros destinos, la dirección técnica del laboratorio de informática forense en la Unidad de Ciberterrorismo. Representante del Instituto armado ,en esta materia, ante diversas organizaciones policiales internacionales, ha desarrollado también una intensa actividad académica y de colaboración con los sectores público y privado en la lucha contra el cibercrimen.

ÁNGEL BODOQUE AGREDANO

Es miembro de la Carrera Fiscal de España desde 1992. A partir de 2006 pasó a formar parte de la plantilla de la Fiscalía Especial Antidroga de la Audiencia Nacional, con sede central en Madrid. En la actualidad desempeña en la Fiscalía todos los ámbitos de trabajo ordinarios, y de forma más intensa es el Coordinador del Servicio de Cooperación Internacional de dicha Fiscalía, Corresponsal Nacional de Eurojust para asuntos de Salud Pública y Punto de Contacto de EJN, IBERRED y la Red de Fiscales Antidroga de Iberoamérica, así como Representante de España en el Grupo de Trabajo de la AIAMP sobre Lavado de Activos y Economía Criminal.

Edición no venal
Madrid, abril de 2022

No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Esta publicación ha sido elaborada con la financiación de la Unión Europea. Su contenido es solo responsabilidad del programa "EL PAcCTO" y no refleja necesariamente las opiniones de la Unión Europea.

CONTENIDO

SÍNTESIS DE LA GUÍA

La primera parte de la Guía ofrece una información sobre los recientes impulsos, fundamentalmente en 2021, después de un período difícil con la pandemia Covid-19, en el ámbito internacional, singularmente a través de las actuaciones del GAFI, y de las Propuestas de trabajo de la Unión Europea en relación con un paquete importante de medidas de lucha contra el blanqueo de capitales, que tienen como objetivo, entre otras, actuaciones de supervisión más estrictas relativas a la utilización de criptoactivos en el sistema financiero, y cuando se produce su aparición en el sistema represivo penal, las respuestas desde la Jurisdicción.

Junto a lo anterior, se expone el ejemplo español con la reciente adaptación legal de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (Quinta Directiva). Aquí destaca el doble objetivo de perfeccionar los mecanismos de prevención del terrorismo y de mejorar la transparencia y disponibilidad de información sobre los titulares reales de las personas jurídicas y otras entidades sin personalidad jurídica que actúan en el tráfico jurídico. Pero dentro de las modificaciones derivadas de la transposición de la Quinta Directiva es de reseñar la incorporación de nuevos sujetos obligados y, en particular, el sometimiento a las obligaciones preventivas de las personas que presten servicios de cambio de moneda virtual por moneda de curso legal. Asimismo, se incorpora como sujetos obligados a los proveedores de servicios de custodia de monederos electrónicos, entendiendo por tales aquellas personas físicas o jurídicas que prestan servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales de manera similar a la de la custodia de fondos o activos financieros tradicionales. En ambos casos, el sometimiento a la normativa de prevención del blanqueo de capitales se acompaña, tal y como requiere la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, de una obligación de registro de estos prestadores. Supone un buen modelo que podría ser exportado al ámbito iberoamericano. A los efectos anteriores, se incluye un cuadro explicativo del resultado de esta nueva legislación en España, que se está valorando en los países americanos del ámbito AIAMP, después de su aprobación reciente en el Grupo de Trabajo de Lavado de Activos y Economía Criminal. Se indicarán también en este punto las consideraciones de algunos Tribunales españoles y europeos sobre la naturaleza jurídica de los Activos virtuales.

Derivado de lo anterior, la naturaleza de los Informes de Inteligencia Financiera sobre operaciones sospechosas en el ámbito de las operaciones con criptoactivos tiene ahora una doble dimensión: en primer lugar la propia actividad de los “vigilantes” de estas operaciones, cuyos incumplimientos pueden dar lugar a responsabilidad penal en este ámbito; en segundo término, la necesidad de que dicha información de inteligencia, al no poder constar en modo alguno en un procedimiento judicial, se incorpore como otra información más, pero cualificada, en la actividad investigativa de los operadores policiales, al objeto de ser presentada debidamente a la Autoridad judicial de la investigación del delito de Lavado de Activos mediante criptomonedas.

Por su interés y en cuanto a la consideración de renovados conceptos en el uso de la Información financiera para la prevención, detección, investigación y enjuiciamiento de infracciones penales, con relación directa respecto de actividades de la Delincuencia organizada de Lavado de Activos, se harán unas breves indicaciones sobre la nueva normativa que supone la Directiva 2019/1153 de la UE, la llamada Directiva de la Información financiera a nivel policial, pendiente de transposición por algunos países de Europa como España.

En esta parte de la Guía se exponen también, descendiendo a un nivel práctico, derivado de

casos reales de Investigación Penal, algunas tipologías recientes detectadas con elemento de conexión Iberoamérica o ámbito AIAMP, donde se aprecian las vulnerabilidades y las posibilidades del uso de criptoactivos o activos virtuales como medio o instrumento de la actividad de Lavado o blanqueo de capitales. Se trata de una información obrante también en el Grupo de Trabajo de la AIAMP sobre Lavado de Activos y Economía Criminal.

Por último, se expondrán algunos ejemplos concretos de Medidas cautelares adoptadas en los procedimientos judiciales sobre la aprehensión y puesta a disposición de los criptoactivos intervenidos o bloqueados provisionalmente por las autoridades judiciales en los procedimientos de investigación, estableciendo varios Anexos, que se pueden utilizar en el ámbito interno de cada país con las necesarias adecuaciones, al margen de la Guía propiamente dicha, y que pueden ser de utilidad en la actividad operativa jurisdiccional, siempre con adaptación a la legislación nacional respectiva en función de la regulación de los Códigos Penales Procesales.

La segunda parte de la Guía ofrece una visión general y unos conceptos básicos que permitan una primera aproximación al mundo de las criptodivisas. Se pretende abordar esta temática de una manera conceptual, no técnica, y centrada en los aspectos prácticos que permitan entender el funcionamiento, la metodología, amenazas y usos que se detectan en el contexto del blanqueo de capitales con criptodivisas desde la perspectiva policial.

Se procederá a describir y definir las criptodivisas, los diferentes actores involucrados para su obtención, su uso, trazabilidad y, lo más relevante en el aspecto que nos ocupa, las distintas metodologías utilizadas para llevar a cabo actividades de blanqueo de capitales.

Describiremos los elementos utilizados para la facilitación del lavado de activos con criptomoneda, sus vulnerabilidades, así como distintos aspectos en relación a las monedas virtuales, independientemente de la legislación aplicable.

Para afrontar el reto que supone la investigación policial de cualquier modalidad delictiva que incluye el uso de criptoactivos es preciso realizar ciertas adaptaciones en las estructuras policiales que permitan reaccionar de forma adecuada ante esta amenaza. Veremos ciertas recomendaciones y buenas prácticas sobre este aspecto.

Por último, se reflexiona sobre los retos futuros y la posible evolución del uso de los criptoactivos en el marco de estudio.

La guía pretende ser una primera referencia básica sobre investigación en el lavado de activos con criptodivisas, debiéndose dirigir a manuales más específicos si se precisa profundizar en algún tema en concreto.

CONTEXTO

La vertiginosa revolución tecnológica que vivimos llega a todos los rincones de nuestra sociedad. El mundo de las finanzas, y el comercio no es ajeno a esta evolución. Vemos continuamente la aparición de nuevas formas de realizar transacciones, nuevos espacios de comercio virtual, novedosos medios de pago e incluso nuevas formas de representar el dinero, más allá del concepto tradicional. Estos cambios, ya no debieran sorprender a nadie, son aprovechados de manera inmediata por los delincuentes para favorecer sus actividades creando nuevas modalidades delictivas vinculadas a estas tecnologías.

EL aprovechamiento de los beneficios obtenidos por actividades delictivas ha encontrado en el nuevo ecosistema financiero virtual una nueva forma de conservar, transferir, ocultar, y dar salida a esos activos mediante lavado en criptodivisas.

Resulta un reto nada sencillo de abordar el dar una respuesta policial a tales actividades, exigiendo una rápida adaptación, creación de estructuras y dotación de medios y de formación adecuada a agentes especializados.

Para esto es importante conocer, aunque sea de forma superficial, que actores intervienen en este nuevo ecosistema virtual y que impacto tiene cada uno en la consecución del lavado de capitales.

El marco jurídico preventivo y el represivo penal frente a la realización de conductas favorecedoras del Lavado de Activos mediante Criptoactivos ha tenido un vertiginoso desarrollo también en los últimos tiempos, y por ello en el presente documento se hace un estudio de las novedades y futuros desarrollos legales en esta materia, que, aunque circunscritos al ámbito europeo, pueden ser adoptados en un futuro modelo por legislaciones y prácticas iberoamericanas, en la medida en que todos los planteamientos legislativos tienen también como fuente las normas más internacionales de los organismos referencia en este ámbito, singularmente el Grupo de Acción Financiera Internacional.

DESARROLLO

Impulsos internacionales recientes para la persecución del Lavado de Activos mediante Activos virtuales

El resumen del panorama internacional en la lucha contra el Lavado de Activos ha sido identificado en el año 2021 de una manera clara por la Estrategia de lucha contra la Delincuencia Organizada 2021-2025 de la Unión Europea: "Pese a los avances de los marcos jurídicos destinados a luchar contra el blanqueo de capitales y recuperar activos, solo se detecta un pequeño porcentaje de las actividades de blanqueo de capitales, y únicamente se confisca el 1 % de los activos de origen delictivo. Esta situación se ha agravado con el uso cada vez mayor de canales financieros sometidos a una vigilancia más limitada que la del sector bancario, como las monedas virtuales."

Son las normas de prevención del blanqueo de capitales las más preocupadas en los últimos tiempos por la utilización de las monedas virtuales como medios de pago y las transacciones ilícitas. Así, La Directiva 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Diario Oficial de la Unión Europea L 156/43, 19 de junio de 2018, define la moneda virtual, a la que se adscribirían las criptomonedas, como *"representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos".*

Antes de la anterior, el Art. 2 de la Directiva 2014/62/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo. Diario Oficial de la Unión Europea L 151/1, 21 de mayo de 2014, consideraba que las criptomonedas no podían ser consideradas monedas de curso legal, en una interpretación más antigua y más desligada del enorme desarrollo de este tipo de Activos.

Hoy de nuevo, la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo. Diario Oficial de la Unión Europea L 123/18, 10 de mayo de 2019, vuelve a hablar de las monedas virtuales como *"representación digital de valor que no ha sido emitida ni está garantizada por un banco central ni por una autoridad pública, no está necesariamente asociada a una moneda de curso legal ni posee la condición jurídica de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos".*

La consolidación del concepto y sistema de "blockchain" abre nuevas posibilidades a la criminalidad informática y de manera transversal fortalece las actividades de Lavado de Activos de origen criminal en todas sus modalidades.

El panorama legal pretende ser fortalecido y aclarado a través de recientes impulsos, por un lado el propio GAFI, después de su Reunión Plenaria reciente del mes de Octubre de 2021 en París, y de nuevo por la propia Unión Europea, con todo un paquete de medidas legislativas de lucha contra el blanqueo de capitales, que pretenden el objetivo de reforzar el marco preventivo de LBC/LFT en la UE mediante la eliminación de las lagunas aún existentes que permiten a los delincuentes hacer un uso indebido del sistema financiero de la UE para blanquear su producto

ilícito o hacen posible la financiación del terrorismo a partir de sus actividades terroristas.

Ese objetivo lo espera conseguir la UE "gracias a una actuación en los ámbitos legislativo y estructural:

- *Un conjunto más claro de normas, incluidas disposiciones directamente aplicables, lo que garantizará una aplicación más coherente del marco. Esto proporcionará un planteamiento más coherente a aquellas entidades que tienen que aplicar las normas de LBC/LFT en la UE, así como en relación con las medidas que estas deben poner en práctica, además de introducir un límite máximo para los pagos en efectivo en la UE.*
- *La creación de una Autoridad Central en LBC para la UE, la cual mejorará la supervisión y respaldará la cooperación entre las UIF."*

A tenor de lo anterior, dicho paquete legislativo se compone de los trabajos siguientes:

- *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo*
- *Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se deroga la Directiva (UE) 2015/849*
- *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010.*
- *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos.*

Respecto de esta última, que es la que más nos puede ahora interesar a los efectos de este trabajo, el documento señala que "con el fin de prevenir, detectar e investigar su posible uso para el blanqueo de capitales y la financiación del terrorismo, se adoptó el Reglamento (UE) 2015/84713 para asegurar la plena trazabilidad de las transferencias de fondos, garantizando la transmisión de información a lo largo de la cadena de pagos mediante el establecimiento de un sistema que impone a los proveedores de servicios de pago la obligación de acompañar las transferencias de fondos con información sobre el ordenante y el beneficiario. Sin embargo, actualmente el Reglamento (UE) 2015/847 solo se aplica a las transferencias de fondos, que se definen como «los billetes y las monedas, el dinero escritural y el dinero electrónico» en el artículo 4, punto 25, de la Directiva 2015/2366 del Parlamento Europeo y del Consejo14, y no a la transferencia de activos virtuales. De hecho, hasta 2018 no se adoptaron nuevas normas internacionales para establecer un requisito de intercambio de información en la transferencia de activos virtuales de la misma naturaleza que los existentes para el intercambio de información en la transferencia de fondos." Establecido lo anterior, el proyecto de Reglamento extiende su regulación a las transferencias de activos virtuales. Y concreta alguna de las medidas a implantar, que tendrán su repercusión sin duda como fuente de información en los procesos de investigación penal de conductas delictivas de lavado o blanqueo de capitales utilizando este tipo de criptomonedas, por ejemplo:

- *El régimen de transparencia ya desarrollado para los proveedores de servicios de pagos para la transferencia de fondos a los proveedores de servicios de activos*

virtuales (PSAV) que procesan las transferencias de activos virtuales. La presente propuesta tiene por objeto introducir en el Derecho de la UE estos nuevos requisitos para los PSAV mediante el establecimiento de la obligación de que estos actores recopilen y hagan accesibles los datos relativos a los originantes y a los beneficiarios de las transferencias de activos virtuales o criptoactivos que lleven a cabo.

- *Lo anterior, en coherencia con las propias recomendaciones del GAFI, en sus definiciones de "activos virtuales", como "criptoactivos", y en la de proveedores de servicios de activos virtuales.*

En relación con la actuación del **GAFI**, ya sabemos que se realizó una modificación en junio de 2019 en la Recomendación 15 sobre nuevas tecnologías del Grupo de Acción Financiera Internacional (GAFI) con el fin de incluir los «activos virtuales» y los «proveedores de servicios de activos virtuales», y en particular las nuevas obligaciones en materia de información para los PSCA (Proveedores de Servicios de Activos Virtuales, siglas en inglés) originantes y beneficiarios en cada uno de los extremos de las transferencias de criptoactivos (la denominada «regla de viaje»). Junto a la anterior, la Recomendación 16 ya apuntaba y adelantaba esa novedad en el paquete UE que hemos expuesto con anterioridad, ya que en el caso de las operaciones que impliquen transferencias de criptoactivos, a todas las transferencias de criptoactivos se les debe aplicar los mismos requisitos que a las transferencias electrónicas transfronterizas, en lugar de los aplicados a las transferencias electrónicas nacionales, habida cuenta de los riesgos asociados a las actividades de criptoactivos y a las operaciones de los PSCA, aunque todavía esa recomendación no menciona expresamente las transferencias de criptoactivos como modalidad de transferencia electrónica transfronteriza, que es en realidad lo que constituye la misma.

La novedad como indicábamos al inicio en este año 2021, después de la Reunión Plenaria de París del pasado mes de octubre, lo constituye el impulso de un nuevo enfoque del riesgo renovado que suponen los activos virtuales y los proveedores de servicio en este ámbito. Al respecto, se documenta la necesidad de actualizar su Guía de 2019 para incluir todo el sector de los Activos Virtuales y los Proveedores de Servicios de estos Activos. Se aprecia una coherencia con la política en esta materia puestas en marcha por la Unión Europea a través de ese paquete legislativo de cara al futuro.

El ejemplo español con la transposición de la Directiva 2018/843. Un nuevo sistema de control de las operativas de vigilancia con Activos Virtuales

La Sentencia del Tribunal Supremo de 20 de junio de 2019, resolviendo en casación un asunto patrimonial clásico de estafa, aunque con el elemento del bitcoin como novedad del medio u objeto del delito, indicó que las criptomonedas no eran dinero de curso legal. En consonancia con la decisión del Banco Central Europeo de 2015, califica este activo como un activo patrimonial inmaterial de contraprestación o intercambio en aquellas transacciones bilaterales en las que los contratantes lo acepten. Sin mencionar otro antecedente, en el ámbito del Tribunal de Justicia de la Unión Europea, y bien cierto que, para un asunto de carácter mercantil con derivaciones en las exenciones del IVA comunitario, en la STJUE de 22 de octubre de 2015, el Tribunal Europeo se pronunció sobre el bitcoin calificándolo como medio de pago casi en exclusiva, tratándose de una divisa virtual.

El Tribunal Europeo concretaba que *"La divisa virtual «bitcoin» forma parte de las divisas virtuales denominadas «de flujo bidireccional», que los usuarios pueden comprar y vender con arreglo al tipo de cambio. Por lo que respecta a su uso en el mundo real, estas divisas virtuales son análogas a las demás divisas intercambiables, y permiten adquirir bienes y servicios tanto reales como virtuales. Las divisas virtuales se distinguen del dinero electrónico, tal como lo*

define la Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267, p. 7), en la medida en que, a diferencia de este dinero, en el caso de las divisas virtuales los fondos no se expresan en la unidad de cuenta tradicional, por ejemplo, en euros, sino en una unidad de cuenta virtual, como el «bitcoin».”

El resultado de la transposición comunitaria de la Directiva 2018/843 es en España el Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en diversas materias, entre ellas, la prevención del blanqueo de capitales. Aquí las novedades más importantes se producen, a tenor de la Exposición de Motivos de la norma, en la forma siguiente:

“Dentro de las modificaciones derivadas de la transposición de la Quinta Directiva destaca la incorporación de nuevos sujetos obligados y, en particular, el sometimiento a las obligaciones preventivas de las personas que presten servicios de cambio de moneda virtual por moneda de curso legal. Asimismo, se incorpora como sujetos obligados a los proveedores de servicios de custodia de monederos electrónicos, entendiendo por tales aquellas personas físicas o jurídicas que prestan servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales de manera similar a la de la custodia de fondos o activos financieros tradicionales. En ambos casos, el sometimiento a la normativa de prevención del blanqueo de capitales se acompaña, tal y como requiere la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, de una obligación de registro de estos prestadores”.

Como primera consecuencia, la Ley de Prevención del Blanqueo 10/2010 de 28 de Abril, ha incorporado una definición a sus efectos de los Activos virtuales, con la siguiente indicación en su nuevo artículo 1: «5. Se entenderá por **moneda virtual** aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente. 6. Se entenderá por **cambio de moneda virtual** por moneda fiduciaria la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido. 7. Se entenderá por **proveedores de servicios de custodia de monederos electrónicos** aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales.»

Los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos son ahora sujetos obligados a efectos de la Prevención del blanqueo de capitales, lo que implica la aplicación en bloque de todas las funciones de “vigilancia” en dicho sector, a través de las medidas de diligencia debida. Otra de las consecuencias de la nueva norma es la ampliación de las comunicaciones por indicio en este ámbito de los Activos virtuales, dado que ahora se consideran operaciones por indicio y se comunicarán al Servicio Ejecutivo de la Comisión (la UIF española) los casos que, tras el examen especial, el sujeto obligado conozca, sospeche o tenga motivos razonables para sospechar que tengan relación con el blanqueo de capitales, o con sus delitos precedentes o con la financiación del terrorismo, incluyendo aquellos casos que muestren una falta de correspondencia ostensible con la naturaleza, volumen de actividad o antecedentes operativos de los clientes, siempre que en el examen especial no se aprecie justificación económica, profesional o de negocio para la realización de las operaciones.» La repercusión en el ámbito del Informe de Inteligencia Financiera de una comunicación como la anterior es muy relevante, y podrá ser manejada en el ámbito de la Investigación policial operativa y judicial si así se plantea en el proceso correspondiente.

Un resumen del nuevo régimen español, que ha sido presentado como Ficha denominada **MARCO PREVENTIVO DE LAVADO DE ACTIVOS RESPECTO DE Proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos**

electrónicos, en el Grupo de Trabajo de Lavado de Activos y Economía Criminal de la AIAMP, es el que se puede ver a continuación:

País	España
Fecha de Inclusión	2021 (Real Decreto-ley 7/2021, de 27 de abril, que modifica Ley Prevención de Blanqueo de Capitales y de la Financiación del Terrorismo).
Sujetos Obligados	Los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Las personas o entidades no residentes que, a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente, desarrollen en España actividades de igual naturaleza a las de las personas o entidades citadas Los sujetos obligados quedarán, asimismo, sometidos a las obligaciones establecidas en la presente Ley respecto de las operaciones realizadas a través de agentes u otras personas que actúen como mediadores o intermediarios de aquellos.
Definiciones para la inclusión en la categoría de Sujetos obligados	Se entenderá por moneda virtual aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente. Se entenderá por cambio de moneda virtual por moneda fiduciaria la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido. Se entenderá por proveedores de servicios de custodia de monederos electrónicos aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales.
Medidias normales de diligencia debida	Identificación formal. Identificación del titular real. Propósito e índole de la relación de negocios. Seguimiento continuo de la relación de negocios. Aplicación de las medidas de diligencia debida. Aplicación por terceros de las medidas de diligencia debida.
Medidas simplificadas de diligencia debida	En casos de riesgo reducido de blanqueo de capitales o financiación del terrorismo.
Medidas reforzadas de diligencia debida	No previstas expresamente para Empresas de criptomonedas, pero posibles en función de la valoración de un riesgo elevado de blanqueo de capitales.

País	España
Obligaciones de información	Examen especial de operaciones. Comunicaciones por indicios. Abstención de ejecución. Comunicación sistemática.
Conservación de documentos	SÍ, 10 años.
Protección de datos en el cumplimiento de las obligaciones de diligencia debida	SÍ, los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida no podrán ser utilizados para fines distintos de los relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo sin el consentimiento del interesado, salvo que el tratamiento de dichos datos sea necesario para la gestión ordinaria de la relación de negocios
Productos u operaciones propicias al anonimato y nuevos desarrollos tecnológicos.	Los sujetos obligados prestarán especial atención a todo riesgo de blanqueo de capitales o de financiación del terrorismo que pueda derivarse de productos u operaciones propicias al anonimato, o de nuevos desarrollos tecnológicos, y tomarán medidas adecuadas a fin de impedir su uso para fines de blanqueo de capitales o de financiación del terrorismo. En tales casos, los sujetos obligados efectuarán un análisis específico de los posibles riesgos en relación con el blanqueo de capitales o la financiación del terrorismo, que deberá documentarse y estar a disposición de las autoridades competentes.
Protección de las personas denunciantes dentro de la empresa de Criptomonedas	Las personas expuestas a amenazas, acciones hostiles o medidas laborales adversas por comunicar por vía interna o al Servicio Ejecutivo de la Comisión comunicaciones sobre actividades relacionadas con el blanqueo de capitales o la financiación del terrorismo podrán presentar una reclamación ante el Servicio Ejecutivo de la Comisión (UIF española).
Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos.	SÍ, las personas físicas o jurídicas que, cualquiera que sea su nacionalidad, ofrezcan o provean en España servicios de los descritos en los apartados 6 y 7 del artículo 1 de la ley, deberán estar inscritas en el registro constituido al efecto en el Banco de España. Se inscribirán asimismo en el registro: a) las personas físicas que presten estos servicios, cuando la base, la dirección o la gestión de estas actividades radique en España, con independencia de la ubicación de los destinatarios del servicio. b) Las personas jurídicas establecidas en España que presten estos servicios, con independencia de la ubicación de los destinatarios.

En el ámbito de la vigilancia de estos nuevos sujetos obligados, la situación derivada de esta adaptación normativa, que crea un Registro obligatorio de estos prestadores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos, y cuyo incumplimiento puede ser una infracción muy grave de la legislación antiblanqueo, tiene su cierre del círculo en la consideración de la posibilidad de incurrir en responsabilidad penal por parte de estas entidades, dado que después de la Ley Orgánica 6/2021, en aplicación de nuevo de otra norma comunitaria, la Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal, **puede investigarse a sujetos obligados conforme a la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo, que cometan cualquiera de las conductas descritas en el artículo 301 del Código Penal en el ejercicio de su actividad profesional, esto es, cualquiera de las conductas de blanqueo de capitales en el ejercicio de esta actividad de vigilancia de la operativa con Activos Virtuales, incluyéndose aquí las actividades intencionales en sus diversas modalidades, las cometidas por imprudencia grave, y las realizadas total o parcialmente en el extranjero. Esta responsabilidad penal no solo alcanza directamente a la persona física, sino también a la persona jurídica Sociedad o cualquier otra forma de entidad mercantil cuyo objeto de negocio, como sujeto obligado, sea el de prestador de servicio de cambio de moneda virtual o de custodia de monederos electrónicos, con aplicación de nuevo en bloque de toda la normativa de responsabilidad penal de la persona jurídica.**

Esta previsión anterior supone una ampliación muy importante de la represión penal , y una actualización indudable, abarcando de manera general cualquier actividad favorecedora del blanqueo de capitales a través de los negocios en el ámbito de los Criptoactivos, más allá de la previsión que se incluía en el Código Penal español desde 2015 en relación con actividades de blanqueo que podían favorecer solo la financiación del terrorismo por los sujetos obligados, reducida a los supuestos de imprudencia grave en las actividades de prevención, restricción del tipo penal que hacía prácticamente inaplicable la posibilidad de represión penal.

Al margen de lo anterior, desde las Autoridades financieras y monetarias se está insistiendo en la urgencia y necesidad de implementar estos controles, incluso con independencia de cualquier otra regulación, como así ha sugerido el propio Banco Central Europeo en su Dictamen del pasado 30 de Noviembre de 2021, sosteniendo que " el reglamento propuesto relativo a los mercados de criptoactivos sería útil desde el punto de vista de la estabilidad sistémica y financiera, a fin de garantizar que el mismo se aplique a las transferencias de criptoactivos lo antes posible, en lugar de esperar a la entrada en funcionamiento del resto del conjunto de medidas contra el blanqueo de capitales y la financiación del terrorismo. Como ha señalado la Comisión, hasta ahora, las transferencias de activos virtuales han quedado fuera del ámbito de aplicación de la legislación de la Unión sobre servicios financieros, lo que expone a los titulares de criptoactivos a riesgos de blanqueo de capitales y financiación del terrorismo, ya que los flujos de dinero ilícito pueden realizarse mediante transferencias de criptoactivos y perjudican la integridad, la estabilidad y la reputación del sector financiero". Junto al modelo español expuesto, el modelo alemán sigue la misma estela.[1]

1 . Por ejemplo, el 1 de octubre de 2021 entró en vigor una ordenanza del Ministerio de Hacienda alemán sobre requisitos reforzados de diligencia debida para la transferencia de criptoactivos [***Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten vom 24. September 2021 (BGBl. I S. 4465)***]. Con arreglo a esta ordenanza, los proveedores de servicios de criptoactivos que transfieran criptoactivos por cuenta de un receptor de órdenes deben transmitir de forma simultánea y segura al proveedor de servicios de criptoactivos que actúe en nombre del beneficiario el nombre, la dirección y el número de cuenta (por ejemplo, clave pública) del ordenante, así como el nombre y el número de cuenta (por ejemplo, clave pública) del beneficiario. El proveedor de servicios de criptoactivos que actúe en nombre del beneficiario deberá asegurarse de que recibe y almacena la información del ordenante y del beneficiario. La trazabilidad completa de las partes implicadas en una transferencia de criptoactivos se concibe como una herramienta para la prevención, detección e investigación del blanqueo de capitales y la financiación del terrorismo, así como para el control de la evasión de sanciones. La ordenanza también exige a las entidades obligadas que garanticen que la información del beneficiario o del ordenante de una transferencia se recopile cuando la transferencia se efectúe desde o hacia un monedero electrónico que no esté gestionado por un proveedor de servicios de criptoactivos, aunque no exista riesgo de transferencia de datos.

La nueva Directiva 2019/1153 de la UE y sus consecuencias en materia de análisis de operaciones con criptomonedas dirigidas al Lavado de activos

La finalidad de esta normativa comunitaria es reforzar la seguridad, mejorar el enjuiciamiento de los delitos financieros, luchar contra el blanqueo de capitales y prevenir los delitos fiscales en los Estados miembros y en toda la Unión, para lo cual señala que es necesario mejorar el acceso a la información por parte de las Unidades de Información Financiera (UIF) y las autoridades públicas responsables de la prevención, detección, investigación o enjuiciamiento de delitos graves, potenciar su capacidad para llevar a cabo investigaciones financieras y mejorar la cooperación entre ellas. Junto a lo anterior, se trata de facilitar el acceso directo e inmediato a la información conservada en los **registros centralizados de cuentas bancarias**, que es a menudo indispensable para el éxito de una investigación penal o para la oportuna identificación, localización e inmovilización de los activos conexos con vistas a su confiscación.

Lo anterior tiene una evidente relación con la intervención de criptoactivos en una investigación y con la necesaria trazabilidad que ello haya podido tener como reflejo en los movimientos de todo tipo en cuentas bancarias, con la consiguiente visión de operaciones sospechosas que deben integrar al final los Informes de Inteligencia Financiera.

Para ello, la Directiva mencionada ha dado un nuevo rumbo a diversos conceptos y categorías de instituciones, que van a ser aplicadas en el futuro en las decisiones de ejecución de este instrumento normativo. Algunos de dichos conceptos definidos ahora de manera nueva son:

- *«registros centralizados de cuentas bancarias»: los mecanismos centralizados automatizados, tales como registros centrales o sistemas centrales electrónicos de consulta de datos.*
- *«información financiera»: todo tipo de información o datos, como datos sobre activos financieros, movimientos de fondos y relaciones comerciales financieras, que ya obren en poder de las UIF utilizable para prevenir, detectar y combatir eficazmente el blanqueo de capitales y la financiación del terrorismo.*
- *«información de naturaleza policial»:*

  i) todo tipo de información o datos que ya obren en poder de las autoridades competentes en el contexto de la prevención, detección, investigación o enjuiciamiento de infracciones penales,

  ii) todo tipo información o datos que obren en poder de autoridades públicas o entes privados en el contexto de la prevención, detección, investigación o enjuiciamiento de infracciones penales, y que esté a disposición de las autoridades competentes sin necesidad de adoptar medidas coercitivas en virtud del Derecho nacional.

  Dicha información puede consistir, entre otros, en registros de antecedentes penales, información sobre investigaciones, información sobre la inmovilización e incautación de activos u otras medidas de investigación o provisionales, e información sobre condenas y confiscaciones.

- *«datos sobre cuentas bancarias»: la siguiente información sobre cuentas bancarias y de pago y cajas de seguridad, contenida en los registros centralizados de cuentas bancarias:*

i) respecto del cliente-titular de la cuenta y de cualquier persona que pretenda actuar en nombre de este: el nombre y los apellidos, complementados bien con los demás datos de identificación requeridos por las disposiciones nacionales que transpongan el artículo 13, apartado 1, letra a), de la Directiva (UE) 2015/849, bien con un número de identificación único,

ii) respecto del beneficiario efectivo del cliente-titular de la cuenta: el nombre y los apellidos, complementados bien con los demás datos de identificación requeridos por las disposiciones nacionales que transpongan el artículo 13, apartado 1, letra b), de la Directiva (UE) 2015/849, bien con un número de identificación único,

iii) respecto de la cuenta bancaria o la cuenta de pago: el número IBAN y la fecha de apertura y cierre de la cuenta,

iv) respecto de la caja de seguridad: el nombre y los apellidos del arrendatario, complementados bien con los demás datos de identificación requeridos por las disposiciones nacionales de transposición del artículo 13, apartado 1, de la Directiva (UE) 2015/849, bien con un número de identificación único y la indicación de la duración del período de arrendamiento;

- *«análisis financiero»: los resultados del análisis operativo y estratégico que ya hayan llevado a cabo las UIF para el desempeño de sus funciones.*

La fortaleza en la posición de las Unidades de Inteligencia financiera, a partir de la Recomendación 29 del GAFI, se consolida en la forma siguiente:

"La Unidad de Inteligencia Financiera realiza una función técnica con la finalidad de detectar operaciones sospechosas que remiten los sujetos obligados. A su vez, participa en la supervisión de los sujetos obligados, complementan la labor de estos dando valor agregado a sus reportes, dinamiza la obtención de información con bases de datos enlazadas internacionalmente a través de la Red Segura del Grupo Egmont. Las exigencias con respecto a la presentación de Reportes de Operaciones Sospechosas (ROS) y el mantenimiento de registros generan datos financieros importantes, muchos de los cuales no pueden ser utilizados fácilmente por las autoridades competentes sin realizar un análisis adicional. Si se pretende que los marcos institucionales ALD de un país sean completamente eficaces, el país debe establecer un sistema confiable y eficiente para procesar, analizar y difundir estos datos.
La urgente necesidad de un análisis de datos eficaz sobre un posible delito financiero explica la importancia cada vez mayor de las UIF's y de sus funciones dentro de los esfuerzos internacionales para prevenir, detectar y entablar una acción judicial contra el lavado de activos."[2]

La plasmación de todo lo anterior, con la finalidad de fortalecer la investigación de operaciones con criptomonedas en el Lavado de Activos, pasa por tanto por una configuración como la reciente realizada en la implementación de los refuerzos de una UIF como la española, a saber en dos actuaciones: de manera directa, la titularidad del Fichero Centralizado de cuentas bancarias, llamado Fichero de Titularidades Financieras, y luego, en la realización de los Informes de Inteligencia Financiera, la recopilación de datos procedentes ahora no solo de los sujetos obligados sino de cualquier otra fuente, remitiendo, en tiempo oportuno, si apreciara la existencia de indicios o certeza de blanqueo de capitales, delitos subyacentes conexos o de financiación del terrorismo, o a petición de las autoridades competentes, el correspondiente informe de inteligencia financiera al Ministerio Fiscal o a los órganos judiciales, policiales o administrativos competentes.

2 . Es una de las consideraciones del último Informe Protocolo de Coordinación de las Investigaciones de Lavado de Activos en Perú, de 2021, realizado en el ámbito de un proyecto de la FIIAPP.

Además, el Anteproyecto de adaptación de la norma europea a la legislación nacional, profundiza más todavía en la fortaleza del manejo de información, muy relevante cuando se trata de las operaciones con Activos virtuales como hemos visto en esta Guía, y por ello incide en desarrollar el acceso directo e inmediato de toda la información de un Fichero Central de cuentas y pagos a todas las Autoridades de la investigación penal. En el fondo, el marco jurídico de la cooperación policial tiene que ser también desarrollado, como base de una excelencia en el uso de la información financiera relevante y la facilitación de la información analizada a las Autoridades jurídicas del proceso de Lavado de Activos.

Algunas tipologías de Lavado de Activos observadas en las concretas investigaciones penales en el ámbito de la región iberoamericana susceptibles de ser realizadas mediante Criptoactivos

En la XXVII Asamblea General de la AIAMP celebrada el 7 y 8 de noviembre de 2019, en Asunción, Paraguay, se acordó la creación del Grupo de Trabajo sobre Lavado de Activos y Economía Criminal coordinado por la Procuraduría General de la Nación de Panamá y conformado por las Fiscalías de Andorra, Argentina, Colombia y España. Además, se han sumado a las labores de este Grupo de Trabajo los Ministerios Públicos de Bolivia, Brasil, Chile, México, Paraguay, Portugal y Uruguay. El Grupo de Trabajo tiene como objetivo facilitar el intercambio de información y buenas prácticas en la investigación de los delitos de Lavado de Activos, así como establecer estrategias conjuntas frente a estos delitos, que, por su naturaleza, tienen un componente transnacional. Para llevar a cabo investigaciones efectivas en contra de los delitos económicos se requiere el trabajo conjunto entre los Ministerios Públicos de la región, propiciando la aplicación de los instrumentos internacionales que brindan las herramientas idóneas para obtener resultados concretos.

Desde el año 2020, el Grupo de Trabajo de la AIAMP sobre Lavado de Activos y Economía Criminal se propone la elaboración y elevación para su aprobación a la correspondiente Plenaria de la AIAMP, de una "**GUÍA DE BUENAS PRÁCTICAS EN LAVADO DE ACTIVOS Y CRIMINALIDAD ECÓNOMICA".**

A falta de su finalización en el primer semestre de 2022, se expone a continuación la aportación en dicha Guía de algunas tipologías recientes observadas en los casos de Lavado de Activos-Blanqueo de Capitales de investigaciones concretas de carácter policial y judicial en el ámbito europeo-español, que tienen como punto de conexión algunos de los países del ámbito AIAMP, y que pretende desarrollar algunas de las menciones que abajo constan realizadas por GAFILAT, sin ánimo exhaustivo.[3] En todas las operativas analizadas, y salvando las específicas con Criptoactivos que se mencionan en epígrafe propio, pueden utilizarse Activos virtuales ya sea como medio de financiación de las operativas, ya como instrumento delictivo de otras actividades delictivas. Todas las operativas permiten la utilización de Criptoactivos y exigen desde este

3 . El Grupo de Acción Financiera de Latinoamérica (GAFILAT) publicó el 21 de septiembre de 2020 un reporte denominado 'Segunda actualización del informe de amenazas regionales en materia de lavado de activos 2017-2018'.
Allí se expone que las tipologías más usadas en la región son el uso de testaferros, seguido de la utilización de personas y estructuras jurídicas, y la transferencia de valores o dinero.
Esta información proviene, en su mayoría, de las evaluaciones nacionales de riesgo de lavado de activos los países integrantes del GAFILAT.
Además, el documento revela que "el sector bancario sigue siendo el sector más vulnerado para lavar activos en la región".
No obstante, también hay un gran impacto en las instituciones públicas, el sector automotriz y el sector inmobiliario, asegura el GAFILAT.
Lavado de activos y delitos fuente
Según el GAFILAT, los países siguen identificando al tráfico ilícito de drogas como la principal amenaza dentro de las evaluaciones nacionales de riesgo.
Sin embargo, llama la atención que ha crecido la percepción de riesgo sobre el delito de contrabando, el cual subió del tercer al segundo lugar en la lista de amenazas.
El tercer lugar, de acuerdo con el informe, lo comparten varios delitos: trata de personas, tráfico ilícito de migrantes, corrupción y soborno.
Haciendo referencia ya a las condenas, la mayoría de ellas tienen como delito determinante el tráfico de drogas.
Algunas señales de alerta
Con base en lo expuesto en el informe del GAFILAT, el "incremento inexplicable de riquezas por parte de personas físicas y uso de testaferros" se pueden considerar como señales de alerta.
Incluso se debería prestar atención a la utilización de servicios de remesas y cambios de divisas, así como las operaciones de comercio exterior para el lavado de activos.

momento la puesta en marcha de todos los recursos de los operadores policiales y judiciales para su detección y persecución.

Compra de inmuebles

Los bienes inmuebles han sido, tradicionalmente, uno de los instrumentos más frecuentes en los esquemas y estructuras de blanqueo de capitales. Las operaciones jurídicas y financieras, las estructuras de propiedad, personales y jurídicas, los instrumentos y medios de pago, la flexibilidad para fijar los precios de intercambio, etc., han hecho de estos bienes un medio especialmente idóneo para el blanqueo de capitales, en cualquiera de sus fases[4].

Un primer cotejo de las operaciones inmobiliarias que han llevado a cabo muchos investigados, algunas utilizando el parapeto de las sociedades, arroja que parecen haberse producido transacciones sospechosas de tratarse de operaciones de blanqueo de capitales, como que **las mismas se perfeccionaran por un precio inferior al de mercado,** ocultando pagos en dinero en metálico que no habría sido declarado **o que los investigados hubieran recurrido a la constitución de préstamos hipotecarios que se valoran como "innecesarios"** teniendo en cuenta la información obtenida a modo de inteligencia financiera que revela la disponibilidad de fondos procedentes del exterior.

Una segunda nota detectada en los últimos tiempos pone de manifiesto en este ámbito la concentración de las operaciones inmobiliarias en un **corto espacio de tiempo**. Tenemos casos donde hemos constatado, que, en un período desde finales de 2017 hasta mediados de 2018, revelan que los investigados afrontaron compraventas de inmuebles por un valor global de 815.0000 euros, en algunos supuestos concretos.

Creación y desarrollo de sociedades instrumentales

El delito de narcotráfico, el subyacente más investigado, constituye una actividad ilícita con un evidente trasfondo económico o patrimonial, generadora de ingentes cantidades de fondos susceptibles de ser blanqueados a través de estructuras societarias dispuestas a tal fin. Así, se observa en multitud de investigaciones cómo los sujetos activos han sido vinculados en un corto espacio de tiempo a más de doce sociedades distintas en España, mostrando mayoritariamente estas mercantiles los rasgos propios de **sociedades instrumentales, bien de carácter patrimonial o del tipo pantalla**.

En este sentido, destacamos el que muchas de las sociedades tengan un **capital social mínimo rondando los 3.000 euros**, que en España es el mínimo de la Sociedad de Responsabilidad Limitada, no habiendo cumplido con la obligación mercantil de depósito de cuentas anuales y, por tanto, aparentemente sin que podamos atribuirle actividad comercial alguna, limitándose en muchos casos a ostentar la propiedad de bienes, especialmente inmuebles con los que transaccionar.

El objeto social de la mercantil constituida es en muchas ocasiones la tenencia, compra y venta de inmuebles y acciones o participaciones de otras sociedades, la gestión y administración de dichos bienes y/o acciones o participaciones de otras sociedades, exceptuándose aquellas actividades de las Sociedades de Inversión Colectiva o que estén sujetas a requisitos especiales por la legislación sobre el Mercado de Valores, dada de alta en el CNAE en el concepto de actividades de las sociedades de Holding. El capital social es el mínimo estipulado por ley, siendo 3.000 €.

Apertura de cuentas bancarias en Europa y posterior movimiento de las mismas en Europa

Esta operativa ha sido siempre utilizada por las organizaciones criminales en general y también por sujetos o grupos más reducidos en particular. Así, se detecta la introducción de importantes sumas de dinero procedente de Sudamérica, que se mezclan con otras transferencias de menor importe de Reino Unido y Estados Unidos, pero todas ellas a la misma cuenta bancaria española. A partir de aquí, se produce el desarrollo de las inversiones en bienes inmuebles, pero

4 . Análisis del SEPBLAC español.

también en la constitución y ampliación de capital de sociedades, ya sean instrumentales, ya sean sociedades que en apariencia tienen operativa real.

Apertura de cuentas bancarias en Europa y posterior movimiento de las mismas en América del Sur

Es una operativa consistente en la apertura de cuentas en entidades financieras españolas, en las que se registran ingresos de fondos, que se disponen con multitud de tarjetas, mediante retiradas de efectivo y compras en comercios, principalmente, en Colombia, sin que el perfil de los titulares de las cuentas justifique este tipo de actividad bancaria.

Se trata del análisis de operaciones de disposición de fondos depositados en cuentas españolas, mediante tarjetas de pago utilizadas en cajeros y comercios colombianos, con los que se consigue trasladar un total superior a los 140 millones de euros, con una estructura que implica a casi 200 mil tarjetas, con sus correspondientes cuentas y personas asociadas.

Estos hechos ponen de relieve el riesgo inherente a la utilización de algunos medios de pago, que deben integrarse en las rutinas de análisis y detección de las entidades obligadas. Esta posibilidad, ya real, de que se esté utilizando la operativa para canalizar hacia el exterior fondos que no tienen origen en una actividad lícita, o, al menos, no en la manifestada por los titulares de las cuentas y tarjetas, que en la inmensa mayoría de los casos no presentan capacidad económica suficiente para justificar los abonos en sus posiciones y la posterior disposición en un país de América del Sur. Además el análisis realizado pone de manifiesto que los fondos tengan como destino un país tradicionalmente relacionado con el narcotráfico, a la existencia de referencias negativas de algunos de los participantes, que les vinculan con actividades delictivas, y, en algún caso, con el tráfico de drogas, y la concurrencia de similitudes en varias de las operativas, que denota una cierta actuación concertada, induce a pensar en la probable vinculación de la operativa con una estructura criminal, internacional y organizada, especializada en la comisión de actividades delictivas, posiblemente relacionadas con el tráfico ilícito de sustancias estupefacientes, y el blanqueo de los beneficios obtenidos, por lo que se propone la judicialización de la investigación.

Ejemplo concreto de esta operativa, se comenta una investigación también de 2018, donde en relación con el uso de tarjetas, la parte de la organización criminal asentada en España dedicada a la venta de sustancias estupefacientes, aportaba grandes cantidades de dinero en efectivo al grupo de blanqueadores, quienes disponían de la infraestructura para llevar a cabo la denominada “bancarización” de dicho dinero. **Este blanqueo de capital se producía mediante el ingreso del dinero en efectivo en pequeñas cantidades en diferentes cajeros automáticos de España, para lo que contaban con una amplia red de testaferros. De manera paralela, miembros de la organización criminal se desplazaban a Colombia con las tarjetas de crédito asociadas a las cuentas corrientes de ingreso, desde donde se realizaban retiradas de efectivo de cajeros automáticos en varias ciudades colombianas como Cali, Bogotá, Medellín y Cúcuta, así como en la ciudad de Panamá[5].**

Movimientos de dinero en efectivo hacia el interior y hacia el exterior, con procedencia o destino de América Central o del Sur

En esta operativa se pone de manifiesto que se trata de un formato de operaciones que, en general, ofrece un riesgo extremo de blanqueo de capitales y financiación del terrorismo. La declaración de los movimientos no tiene impacto económico o fiscal en los declarantes, y la ausencia de declaración produce graves perjuicios por la retirada inmediata del dinero y la importante sanción que suele llevar aparejada. Estas dos circunstancias determinan que los movimientos no declarados se realizan así para ocultarlos a las autoridades españolas o europeas, impidiendo que los datos de una eventual declaración puedan ser incluidos en investigaciones penales o administrativas.

El ejercicio de 2020, frente al de 2019, está afectado por las consecuencias derivadas de la crisis

5 . Fuente: Guardia Civil.

sanitaria. Ha supuesto una variación determinante en las operaciones de salida, que asumen la práctica totalidad de las diferencias en los resultados.

En el ámbito de los movimientos de efectivo de entrada desde América, se ha observado cómo los movimientos son de billetes de alta denominación. Colombia y Bolivia son los países más activos en estos movimientos de llegada de efectivo en 2019 y 2020. En los movimientos de salida hacia América, destacan República Dominicana y Colombia.

Se constata en todo caso, de las investigaciones acaecidas, cómo el año 2020 ha supuesto una caída drástica del transporte de dinero en efectivo de manera irregular, pero no se descarta que vuelva a los niveles de otros momentos en cuanto pase la alarma sanitaria. La asociación de intervenciones de efectivo a investigaciones criminales es mucho más notoria en los transportes internos, dentro del país, y más difícil de identificar en los transportes internacionales.

Tipologías delictivas relacionadas con las monedas virtuales: utilización de las criptomonedas para el blanqueo de fondos de origen ilícito

En este punto hay varias tipologías emergentes, ya aparecidas en investigaciones concretas, pero nos detendremos un poco más en las tarjetas de pago denominadas criptotarjetas.

- **Minería.**

  La obtención de beneficios mediante la práctica de actividades criminales, podría ser empleado por aquellos para la adquisición de equipos de minería, para con ello conseguir el minado de bitcoins, y una vez obtenidos ser reinvertidos en cualquier bien. Hay que tener en cuenta que estos equipos son bastante caros (más de 1.500 dólares por unidad en cualquier página de venta online), muy ruidosos y consumen una gran cantidad de energía. Asimismo el minado de bitcoin, en la actualidad, requiere de una gran capacidad computacional para conseguir minar dicha moneda, por lo que es necesario tener un gran número de estas máquinas funcionando simultáneamente para conseguirlo, conllevando con ello la creación de una gran infraestructura para poder operar con las mismas, debiendo estar dicho lugar insonorizado, además de con gran probabilidad se vinculen o bien a grandes picos de consumo o bien exista un delito conexo de defraudación de fluido eléctrico. Por las características de este tipo de Hardware, actualmente las organizaciones que quisieran invertir en este tipo de instalaciones suelen elegir terceros países para establecer estas granjas de minado, bien porque la electricidad sea más barata o bien porque sean países más fríos y requieran de menor refrigeración, si bien se ha detectado en varias operaciones policiales en España el uso de tal mecanismo para blanquear beneficios ilícitos.

- **Exchangers o plataformas de intercambio.**

  Empresas de intercambio de monedas virtuales por dinero fiduciario y viceversa. Usualmente, estos exchangers dan el servicio de monedero a sus clientes, actuando entonces como entidad depositante de los fondos de su cliente. Se han identificado algunas en América del Sur, porque allí no están sujetas a las limitaciones y restricciones de la Quinta Directiva comunitaria, sobre todo en materia de sujeto obligado en las operaciones. Su ubicación fuera de Europa, por tanto, es un activo para las organizaciones criminales que operan con ellas, o que incluso toman su control, dada las nulas obligaciones de cooperación en el intercambio de información a las autoridades de supervisión. En 2018 ya aparecen investigaciones policiales y judiciales de este tipo, con identificación de los fondos ya blanqueados en Sudamérica.

- **Local Traders.**

  Son personas que se publicitan para llevar a cabo el cambio de moneda virtual a moneda real, en un intercambio p2p (peer to peer). Actúan a modo de los antiguos cambistas de moneda tradicional por divisas o incluso por oro u otros activos. A través de su actividad, que puede ser online, se cambia el efectivo de una actividad criminal.

- **Cajeros Automáticos BTC.**

  Con ello se hace referencia a los cajeros utilizados para poder introducir efectivo y transforma a BTC y enviarla a un determinado monedero del usuario que realiza la operación (y viceversa). Lo ampliamos en apartado diferenciado, dado que ya hay investigaciones activas sobre esta tipología.

- **Tarjetas bitcoin.**

  Básicamente, dichas tarjetas se recargan con BTC y con ellas se pagan en euros o dólares instantáneamente, o bien permite su extracción en efectivo por cajeros de la red bancaria. Estas tarjetas se usan o bien para pagos online o reales a vendedores que no aceptan el pago en criptomonedas, pero sí aceptan el pago con VISA o MASTERCARD, o bien para hacer el cambio de criptomonedas a moneda real a través de cajeros de la red bancaria convencional que sí permiten la extracción con tarjetas VISA o MASTERCARD[6].

Como ejemplo concreto de operación de blanqueo con criptomoneda, en el año 2018, se comenta la siguiente, que tiene una de las operativas aquí mencionadas. Debido a la presión de las entidades bancarias y al rastro que deja este tipo de transacciones, la organización criminal optó por intentar romper esta trazabilidad o seguimiento de sus movimientos de capitales con la compra de criptomonedas, principalmente bitcoins, en una conocida plataforma de venta de moneda virtual. Pese a la dificultad de investigar este tipo de movimientos, la Guardia Civil pudo reconstruir íntegramente toda la trazabilidad del capital gracias a la colaboración judicial con las Autoridades de Finlandia, país de la sede social de la citada casa de cambio, hasta poder determinar el origen y destino del dinero. De esta manera se pudo constatar que todas **las partidas de dinero convertidas en bitcoins procedían de España, concretamente de la organización investigada, y que el destino de las mismas después de las correspondientes operaciones pantalla de compra-venta fueron cuentas corrientes de entidades colombianas**, donde se procedía a la retirada de efectivo en Pesos colombianos. La investigación permitió demostrar el movimiento internacional de efectivo de una organización criminal dedicada al blanqueo de capitales mediante el uso combinado de sistemas de bancarización y movimientos de fondos tradicionales con el de nuevos sistemas como es el mundo virtual de las criptomonedas desde su origen hasta el destino final del dinero en efectivo[7].

Otra operación acaecida en 2019 contempla también **diferentes tipologías** de las comentadas anteriormente en relación con las criptomonedas. Así, se pudo constatar cómo se producían:

- *Recogidas de dinero en efectivo por parte de los denominados "Cash-Carriers" o "Courriers" para su posterior "bancarización" al ingresarlo en cuentas controladas por la organización y su posterior movimiento de fondos entre ellas para dificultar su trazabilidad y control.*

6 . Información de las bases de Europol, contrastada con investigaciones policiales ya activas, sin identificar por protección de datos.

7 . Fuente: Guardia Civil española.

- *Transferencias de grandes cantidades de dinero a cuentas bancarias de sociedades de la propia organización, procedentes de terceras empresas controladas por otros grupos criminales y su posterior salida inmediata al extranjero, principalmente a Exchanges, por lo que se extrae que estarían transformando esos fondos en criptomoneda a través de wallets controlados por el grupo criminal, dificultando su trazabilidad y justificando tales operaciones financieras como "intermediación comercial para la compra de criptomoneda" mediante un negocio real.*
- *Realización de "compensaciones" de dinero en efectivo a través de negocios controlados por la organización, radicados en un lugar muy concreto de un país de Sudamérica.*
- *Uso de testaferros para la apertura y control de sociedades en España, consiguiendo el movimiento de fondos a través de estos negocios y el posible blanqueo de los beneficios obtenidos por su actividad delictiva, así como la ocultación patrimonial, para lo que también empleaban documentación de diferentes personas, suplantándoles la identidad. De hecho, en alguno de los registros practicados, han aparecido DNIs de diferentes personas ajenas a esta investigación, tanto sustraídos como falsificados[8].*

Uso de cajeros ATM bitcoin como evolución de las redes de blanqueo mediante el uso de empresas de gestión de transferencias tradicionales

Se ha detectado como tipología novedosa la utilización de cajeros automáticos de bitcoin pertenecientes a una mercantil concreta, localizados en diferentes puntos de España, por ciudadanos, principalmente de origen sudamericano. La operativa que vendrían desarrollando dichas personas físicas guardaría cierto parecido con la realizada haciendo uso de Empresas de Gestión de Transferencias, , por parte de las redes de blanqueo de capitales, y que es utilizada habitualmente, entre otros, por organizaciones dedicadas al tráfico de estupefacientes. Si bien, añadir, que las ventajas que ofrecen las monedas virtuales, por sus características y funcionamiento, hacen que esta nueva forma de blanqueo mediante su uso ofrezca un mayor grado de anonimidad. Entre las principales características detectadas a partir de las distintas operaciones policiales realizadas en referencia al blanqueo de capitales mediante el uso de EGTS son:

Los envíos son, en su mayoría, realizados por importes que oscilan entre 700 y 1.000 euros, procurando las organizaciones de blanqueo no superar esta cantidad con el fin de evitar el *reporting* sistemático por parte de la gestora de transferencia al Banco Central. El destino de los giros suele ser un mismo país, en Sudamérica. Los envíos de dinero se realizan de manera muy seguida, si bien no se observa regularidad en los envíos. En algunos agentes se observan periodos de tiempo en los que prácticamente no hay actividad con otros en los que el volumen de las operaciones es elevado. Lo que lleva a pensar que el origen de los fondos que se remesan mediante giros se encuentra en entregas elevadas de dinero que posteriormente se fraccionan en múltiples giros originando que la distribución de las remesas pueda ser irregular en función de si la entrada se produce o no y de su cuantía. Existencia de ordenantes que envían dinero en días consecutivos. Un mismo ordenante envía dinero a diferentes personas con las que aparentemente no guarda ninguna relación de parentesco. Los ordenantes en el momento de realizar las operaciones se identifican de forma mayoritaria con el pasaporte de su país de origen. Existencia de concordancia en los volúmenes de actividad o de dinero remesado por parte de diferentes agentes, No existe una explicación lógica que justifique que varios agentes supuestamente independientes entre sí tengan un volumen de operaciones similar mes tras mes y con fluctuaciones importantes de un mes a otro. En cambio, esta operativa se explica si el origen de los fondos es común y se ha realizado un primer fraccionamiento entre los diferentes agentes que controla la organización de blanqueo de capitales y posteriormente un segundo fraccionamiento en múltiples operaciones de envío de dinero o giros.

8 . Fuente: Guardia Civil.
https://bitcoin.org/bitcoin.pdf

Pues bien, ahora esta evolución, con los mismos parámetros, utiliza los cajeros ATM de bitcoin, ya que permiten transformar dinero en efectivo a criptomonedas, para una vez hecho este paso, proceder a realizar diferentes transacciones que dificulten su rastreo, ofreciendo una así mayor anonimidad, y haciendo finalmente uso de EXCHANGES para la recuperación del dinero.

Medidas cautelares de intervención de los Activos Virtuales en los procedimientos judiciales. Conservación, custodia, enajenación anticipada

Aspecto importante de las diligencias de intervención de Activos virtuales en los procedimientos judiciales es la conservación y custodia de algunos de los elementos que conforman los mismos como cuerpo del delito, imprescindible tanto para su utilización en juicio oral como pieza de convicción como para posibilitar la práctica de actos periciales de investigación.

A modo de ejemplo, en el caso español, a tal efecto, los **instrumentos, armas y efectos** a que se refiere el artículo 334 de la Ley de Enjuiciamiento Criminal (en adelante LECr), deben recogerse de forma que se garantice su integridad y acordarse por el juez su retención, conservación o envío al organismo adecuado para su depósito, como determina el artículo 338 de la LECr.

Sin embargo, la misma normativa española indica diversas menciones sobre realización anticipada de los efectos judiciales, que es común a los **efectos del delito**, en sentido estricto, y a los **bienes objeto de medidas cautelares reales**, pues ambos tipos de cosas caben en el amplio y novedoso concepto de efecto judicial, ex artículo 367 bis de la LECr.

La realización anticipada solo puede afectar a **elementos de lícito comercio** que no sean piezas de convicción ni deban quedar a expensas del procedimiento y puede consistir en:

- *La entrega a las Administraciones públicas o a entidades sin ánimo de lucro;*
- *La realización por persona o entidad especializada; o*
- *la subasta pública, pudiendo acudirse a la primera modalidad cuando los efectos sean económicamente irrelevantes.*

La **realización mediante persona o entidad especializada o por subasta** ha de realizarse en la forma prevista en la LECr, previo informe del Ministerio Fiscal y de los interesados, quedando afecto el producto de la venta a la satisfacción de las responsabilidades civiles y costas que se declaren, una vez deducidos los gastos de cualquier naturaleza que se hayan producido. A tal efecto, se ingresa en la cuenta de consignaciones del juzgado o tribunal correspondiente.

Cuando el **bien** de que se trate esté **embargado** en ejecución de un acuerdo adoptado por una **autoridad judicial extranjera** en aplicación de la Ley de Reconocimiento Mutuo, Ley 23/2014, su realización no podrá llevarse a cabo sin obtener previamente la autorización de la citada autoridad.

Puede también autorizarse la **utilización provisional** de los **efectos que no sean perecederos**, cuando concurra alguna de las restantes circunstancias expuestas en la norma, siempre que además se trate de efectos especialmente idóneos para la prestación de un servicio público, o cuando su utilización permita a la Administración un aprovechamiento de su valor mayor que la realización anticipada, o no se considere procedente la realización anticipada de los mismos.

Sigue pendiente la configuración de un sistema integral de Gestión y Administración de Activos virtuales intervenidos, que de momento no es posible a través del ya constituido organismo de gestión y recuperación de activos, hoy denominado en España “Dirección General de Seguridad Jurídica y Fe Pública del Ministerio de Justicia”, dado que la elaboración de un contrato de gestión con entidad externa a estos efectos se encuentra en fase de elaboración. Esta situación está suponiendo que sean los propios Juzgados de la investigación penal quienes están decidiendo

los actos de gestión y administración de los Activos virtuales intervenidos.

Toda la configuración anterior de las medidas cautelares, no debe olvidarse, se dirige fundamentalmente a su garantía para el futuro decomiso de dichos Activos Virtuales, considerando las disposiciones generales y especiales del propio Código Penal a estos efectos, en concreto la principal, a saber:

Artículo 127 del Código Penal:

> *1. Toda pena que se imponga por un delito doloso llevará consigo la pérdida de los efectos que de él provengan y de los bienes, medios o instrumentos con que se haya preparado o ejecutado, así como de las ganancias provenientes del delito, cualesquiera que sean las transformaciones que hubieren podido experimentar.*
>
> *2. En los casos en que la ley prevea la imposición de una pena privativa de libertad superior a un año por la comisión de un delito imprudente, el juez o tribunal podrá acordar la pérdida de los efectos que provengan del mismo y de los bienes, medios o instrumentos con que se haya preparado o ejecutado, así como de las ganancias provenientes del delito, cualesquiera que sean las transformaciones que hubieran podido experimentar.*
>
> *3. Si por cualquier circunstancia no fuera posible el decomiso de los bienes señalados en los apartados anteriores de este artículo, se acordará el decomiso de otros bienes por una cantidad que corresponda al valor económico de los mismos, y al de las ganancias que se hubieran obtenido de ellos. De igual modo se procederá cuando se acuerde el decomiso de bienes, efectos o ganancias determinados, pero su valor sea inferior al que tenían en el momento de su adquisición.*

En la práctica de las causas judiciales actual con la intervención provisional de Activos virtuales, se procede a autorizar a las Unidades Policiales de Investigación a la creación de un monedero virtual, para la transferencia al mismo del dinero virtual hallado en las primeras actuaciones, así como en caso de encontrar en los dispositivos electrónicos la existencia de monederos de cualquier tipo de medio digital de intercambio o criptomoneda, autorizar la intervención de las cantidades existentes en las mismas y su transferencia a este monedero virtual creado por dichas Unidades.

Desmitificando las criptodivisas

Por lo expuesto hasta el momento podría deducirse que la criptomoneda tiene un uso particularmente vinculado al entorno criminal. Sin embargo, recientes estudios demuestran que únicamente alrededor del 1% de todo el valor de las transferencias de criptomoneda están vinculada a actividades delictivas. En todo caso, esto supone unos diez mil millones de dólares.

Si hablamos exclusivamente del lavado de capitales Un pequeño grupo de servicios turbios de criptomonedas, que en su mayoría operan sobre grandes intercambios, realizan la mayor parte del lavado de dinero del que dependen los ciberdelincuentes para rentabilizar los delitos basados en criptomonedas. Tan solo 275 destinatarios de depósitos de servicios controlan el 55% del blanqueo de capitales en criptomonedas.

El auge actual de las criptomonedas, en especial bitcoin, y su presencia en medios de comunicación social, genera mucha confusión debido a la aparición de una nueva terminología. La necesidad de investigar cualquier tipología delictiva basada en esta tecnología hace preciso conocer este nuevo ecosistema de valor virtual. Se deben comprender y distinguir los términos relacionados con criptodivisas, así como comprender y diferenciar a los distintos actores que operan en este entorno.

Dinero digital

Se entiende por dinero digital todo aquel que se usa para pagar algún producto o servicio a través de un medio electrónico, sin tener que utilizar el dinero físico. El dinero digital es, por ejemplo, el que se emplea cuando se realiza una compra con tarjeta de crédito o cuando se realiza una transferencia desde un teléfono móvil utilizando cualquier aplicación de un banco. Por lo tanto, se está usando dinero digital cuando se realiza un pago o envío de dinero sin intercambiar físicamente monedas o billetes.

Esta forma de realizar transacciones le está ganando el terreno al dinero en efectivo. Se estima que la cantidad de dinero efectivo en circulación es aproximadamente solo el 8% del total del dinero existente.

Dentro del concepto de dinero digital, se encuentran también las otras variantes mencionadas anteriormente: la moneda virtual y las criptomonedas, pero que presentan características propias.

Moneda virtual

Este tipo de dinero se podría definir como todo aquel que únicamente existe en un entorno virtual, sin correspondencia con el dinero físico.

Como ejemplos de monedas virtuales se pueden mencionar:

- *El que una empresa para compensar e incentivar a sus empleados, mediante acumulación de puntos.*
- *El que se les asigna a los jugadores de un videojuego con objeto de que lo utilicen para comprar objetos o acceder a otros niveles del juego.*
- *Los programas de fidelización, por ejemplo, el de las aerolíneas que permite la compra de billetes o de otros servicios de la compañía por acumulación de puntos.*

Con objeto de evitar su posible uso delictivo (blanqueo de capitales, financiación de actividades terroristas, …) se ha intentado definir qué es la moneda virtual desde diversos organismos oficiales si bien estas definiciones han estado marcadas por el grado de aceptación de este tipo de moneda en cada momento histórico.

En el marco de la Unión Europea fue el Banco Central Europeo quién en un primer momento abordó su definición en el año 2012 determinando que: "*Una moneda virtual es un tipo de dinero digital no regulado, que es emitido y, generalmente controlado por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual específica"*. Con esta definición podríamos decir que toda moneda virtual es dinero digital, pero a día de hoy esto ya no es así. Varios países han optado por realizar cambios normativos regulatorios, como, por ejemplo, Australia, donde este tipo de moneda ya es considerada como una moneda regular.

Por este motivo, en 2015 el Banco Central Europeo se vio obligado a actualizar la definición de dinero virtual estableciendo que era *"Una representación digital de valor, no emitida por ninguna autoridad bancaria central, institución de crédito o emisor de dinero electrónico reconocido, que, en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero"*. Se pretendía así, diferenciarlo del dinero que se conocía hasta ese momento ajustando la definición al uso de las monedas virtuales en ese momento.

El Parlamento Europeo en su Directiva (UE) 2018/843 y del Consejo, de 30 de mayo de 2018, por la que se modifica la anterior Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo; también conocida como *"Quinta Directiva"* o *"The Fifth Anti-Money Laundering Directive"* (AMLD5), define las monedas virtuales, como: *"Representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos"*.

En esta misma Directiva se establece un control sobre los proveedores de servicio de cambio, entidades que facilitan el cambio de moneda virtual por moneda fiduciaria (FIAT), pues suele ser un lugar aprovechado por organizaciones delictivas y grupos terroristas para el blanqueo de capitales aprovechando el anonimato que ofrecen las monedas virtuales. Asimismo, la propia Directiva permite que las Unidades de Inteligencia Financiera (UIFs) puedan obtener de estas la información necesaria para identificar a los propietarios de las monedas virtuales respetando siempre los derechos fundamentales.

Analizando estas dos últimas definiciones se llega a la conclusión de que la moneda virtual no posee el mismo estatus que una moneda FIAT y, además, no cuenta con ningún tipo de control y respaldo de los bancos centrales. Sin embargo, teniendo en cuenta la teoría monetaria clásica, las utilidades de la moneda virtual guardan cierta similitud con las del dinero fiduciario en tanto que, según esta, dinero es todo aquel bien que se pueda emplear como medio de pago, unidad de cuenta y depósito de valor.

La característica del medio de pago consiste en su uso para poder efectuar una transacción, lo que genera un intercambio de servicios, bienes y productos. Es decir, se recibe una cosa a cambio de otra y el medio de pago utilizado cuenta con un reconocimiento dentro de una comunidad de usuarios. Este medio de pago tiene un depósito de valor o reserva de poder adquisitivo, de modo que, se transfiere el poder de compra del presente al futuro. El individuo que recibe el dinero es consciente de que en el futuro podrá hacer uso de ese dinero para comprar otros bienes o servicios. Las personas no quieren el dinero de por sí, sino para poder cambiarlo posteriormente por otros bienes y porque ese dinero será aceptado por otras personas en el futuro. Por ejemplo, cuando se compra un producto en un establecimiento, el vendedor que recibe el dinero lo puede guardar y convertirse en un futuro comprador en cualquier momento.

En este contexto la moneda virtual puede ser empleada como medio de pago o cambio en comercios o tiendas que así lo tengan establecido igual que el dinero físico. Sin embargo, el hecho de que a la moneda virtual se le pueda atribuir las mismas funciones que al dinero en términos económicos, no significa que tengan la misma consideración desde un punto de vista legal.

Criptodivisa

La criptodivisa o criptomoneda es un medio digital de moneda virtual, convertible y descentralizada. Todo dinero digital que está protegido por criptografía se denomina criptodivisa o, por su terminología más común, criptomoneda.

Así como el dinero digital y el virtual tienen varios años de existencia, la criptomoneda es bastante más reciente. Se cataloga dentro de las monedas virtuales y tiene la gran ventaja de que se encuentran protegidas por diversos mecanismos de criptografía. La encriptación es el proceso de codificar un mensaje o información de tal manera que solo las partes autorizadas puedan acceder a él. Existen diferentes tipos de cifrado: bien mediante esquemas de clave simétrica, bien por clave asimétrica (también llamada de par de claves pública-privada).

Una de las grandes novedades de las criptomonedas es que no cuentan con un emisor concreto a diferencia del dinero FIAT, y que sus operaciones no están controladas por ningún intermediario, ya que son los propios usuarios, a través de un software de código abierto y la implementación criptográfica, los que facilitan la seguridad y el anonimato de todo el sistema distribuido. Podemos decir que todas las criptomonedas son monedas virtuales y dinero digital, pero no a la inversa.

Dado el gran abanico de criptomonedas existentes, y teniendo en cuenta que bitcoin es la más conocida al ser la primera en entrar en el mercado, a partir de ahora nos centraremos principalmente en esta. Bitcoin ocupa la primera posición del mercado de las criptomonedas seguida del Ether de la blockchain Ethereum. El ***paper*** -artículo científico de ámbito académico- que presentaba las bases teóricas del bitcoin fue publicado el 1 de noviembre de 2008 por Satoshi Nakamoto[9]. En ese artículo se presenta una nueva tecnología basada en la criptografía llamada blockchain, con la que se pretende crear un método de pago descentralizado entre usuarios, sin

9 . Los intercambiadores también son conocidos como ***Virtual Asset Service Providers*** (VASPs).

la necesidad de contar con entidades financieras que controlasen las transacciones.

Bitcoin y la tecnología blockchain

Bitcoin emplea la tecnología blockchain, también conocida como cadena de bloque o libro de contabilidad distribuido. De forma sencilla, se puede definir la cadena de bloque como una base de datos donde quedan registradas todas las transacciones agrupadas en forma de bloques entrelazados entre sí, otorgando al sistema transparencia y seguridad.

Desde el punto de vista jurídico esta tecnología se define como: *"Un sistema distribuido de registros contables entre iguales que usa un algoritmo que negocia la información contenida en esos registros en bloques de datos ordenados y conectados junto con tecnologías criptográficas y de seguridad para alcanzar y mantener la integridad de los mismos"*.

La tecnología Blockchain, utilizada en bitcoins y otras monedas virtuales, tiene una importante ventaja respecto a otras tecnologías existentes, ya que contribuye a lograr una mayor integración financiera mundial:

- *Permite el acceso global a un nuevo sistema de pagos a cualquier persona con acceso a Internet, lo que hace posible los pagos internacionales para casi todos los habitantes del planeta, sin hacer uso del sistema financiero y las redes bancarias existentes.*

  Esta accesibilidad ofrece enormes ventajas a las empresas legítimas que desean ofrecer sus productos y servicios en línea y a quienes desean comprarlos. Los esquemas actuales de dinero electrónico pueden transferir dinero casi instantáneamente. Estos sistemas ofrecen a los usuarios la posibilidad de almacenar fondos de forma segura y de transferirlos a cualquier lugar del mundo de forma considerablemente más rápida y barata que antes.
- *Las monedas virtuales creadas con la tecnología Blockchain también pueden personalizarse ex ante, lo que hace que el sistema sea menos dependiente de las políticas monetarias centralizadas. Esto significa que las transacciones no pueden revertirse, solo pueden ser reembolsadas por la persona que recibe los fondos. Las criptomonedas, a diferencia de muchos sistemas de dinero electrónico regulados, no ofrecen un proceso de escalada que los clientes puedan utilizar para presentar una reclamación en caso de disputa en relación con una transacción.*
- *Por último, los costes de las transacciones suelen ser menores, ya que el único coste es una pequeña tarifa por el uso de la red y el proceso de minado.*

Ejemplo de transacción

Para realizar una transferencia a través de una entidad bancaria convencional, es necesaria la presencia de intermediarios. Por ejemplo, si Alberto quiere transferir 100 € a Carlos, la entidad bancaria de Alberto es la que se encarga de hacer llegar los 100 € a la entidad bancaria de Carlos. Una vez el banco de Carlos recibe la notificación, se ingresa el dinero en su cuenta. Dependiendo de los bancos y los países, esta operación puede demorarse minutos o incluso días. Se puede observar, que se trata de una operación muy sencilla, si bien Alberto y Carlos no tienen ningún tipo de control en la operación, pues han depositado su confianza en las entidades bancarias.

Con la creación de la tecnología de cadena de bloque se busca básicamente acabar con la presencia de intermediarios, es decir, de los bancos, dejando registradas todas las operaciones que se realizarán en la cadena de bloque. Lo que antes se conocía como banco, ahora se ha convertido en una red compuesta por usuarios, que se le dará el nombre de "nodos". Estos nodos serán los encargados de verificar de forma simultánea cada una de las transacciones que se realicen en el sistema. Una vez el bloque alcanza un número de transacciones predeterminadas, este se cierra y se empieza uno nuevo.

Recordando el ejemplo anterior, si Alberto en vez de 100 €, le envía 1 bitcoin a Carlos, los pasos que tendría la operación empleando la cadena de bloques, serían:

1.Alberto le expone a la red que quiere enviar 1 bitcoin a Carlos.

2.Los nodos de la red anotan la solicitud de Alberto para posteriormente poder asegurarse de que Alberto tiene ese bitcoin en su cartera.

3.Al mismo tiempo, se van anotando en el mismo bloque otras transacciones ajenas a la de Alberto y Carlos.

4.Se registra en el bloque la transacción de Alberto y Carlos junto con las otras anotadas.

5.Una vez el bloque alcanza el límite de transacciones, los nodos de la red tendrán que verificar que todas las transacciones anotadas se han añadido al bloque y a continuación sellarlas, entre ellas la transacción de 1 bitcoin entre Alberto y Carlos.

6.Por último, una vez los bloques estén válidos y sellados, se incorporan a la cadena de bloque de forma definitiva e inalterable.

A grandes rasgos así sería cómo se realiza una transacción a través de la cadena de bloque. En la realidad, la red no sabe quién son Carlos y Alberto, sino que se emplea una criptografía asimétrica con la que se pretende alcanzar la seguridad y la confidencialidad que caracteriza a las criptomonedas.

La criptografía asimétrica es un sistema de criptografía que emplea dos claves, una clave pública y una clave privada, que dan control al acceso de los bitcoins que se tengan almacenados en un monedero. Ambas claves están relacionadas entre sí, pues la clave pública se genera a partir de la clave privada.

- *La clave pública, también conocida como dirección bitcoin, será lo equivalente al número de cuenta bancaria y puede ser conocida por todos los usuarios, ya que se emplea para recibir bitcoin.*
- *La clave privada, será lo más parecido a un número PIN secreto que dará acceso a las criptomonedas almacenadas, por lo que únicamente deberá de ser conocida por su propietario. La clave privada será necesaria para firmar transacciones o para autorizar cualquier movimiento de nuestros bitcoins.*

Destacar que la cadena de bloque es pública y puede ser consultada por cualquier usuario para cerciorarse del correcto funcionamiento del sistema.

En resumen, la cadena de bloque es *"un bien inmaterial mueble, digital, no fungible, en forma de documento electrónico, susceptible de propiedad privada y gestionado informáticamente a través de una clave pública y otra privada, descentralizadamente, sin Autoridad de emisión o control, apoyada en una red de distribución persona a persona, a través de nodos interconectados (ordenadores/usuarios) que verifican colectivamente las transferencias."*. Por lo que esta tecnología se asegura un sistema descentralizado, seguro y transparente que evita problemas de duplicidad.

Principales características de las criptomonedas

Tres elementos importantes que diferencian las criptomonedas: Seguridad, descentralización y anonimato.

- **Seguridad**

  La seguridad se obtiene a través de la función resumen, también conocida como función hash, que la proporciona el propio cifrado. La función hash no es

más que un algoritmo matemático que resume los datos de las transacciones en una serie de caracteres de longitud fija. En el momento en el que se vea alterado algún dato almacenado en la cadena de bloque, el hash se vería modificado.

Con la aplicación de estos algoritmos matemáticos el sistema se asegura que no se producen modificaciones indeseadas por terceros y se garantiza la integridad y la inalterabilidad de las criptomonedas. A través de la función hash se dificulta un posible hackeo del sistema y se repelen todos los ataques que intentan debilitar las medidas de protección establecidas.

Cuando una transacción se incorpora en el bloque, esta se sella y se une a la siguiente, dotando a la transacción de seguridad frente a posibles fraudes, como el doble gasto, a diferencia de otras monedas digitales clásicas (p.ej. las tarjetas de crédito), que están expuestas a posibles falsificaciones y donde puede originarse el problema del doble gasto.

En resumen, todos los problemas de seguridad que se pueden presentar han sido convenientemente resueltos con la arquitectura de bloque y el cifrado.

- **Descentralización**

La segunda característica principal de las criptomonedas es la descentralización, que es la gran diferencia entre las criptomonedas y las formas de pago tradicionales, donde todas las operaciones realizadas se anotan en un único servidor, aunque se realicen copias de seguridad en otros servidores como salvaguarda.

“A diferencia de las redes centralizadas que necesitan diferentes tipos de certificadores, las redes descentralizadas dependen de la confianza de los pares y utilizan mecanismos de consenso para mantenerse y actualizarse.”

Con la tecnología de blockchain, a medida que se van realizando transacciones, estas se agregan en bloques, que se van añadiendo a un libro contable repartido entre múltiples nodos sin la necesidad de requerir autoridades que aprueben o ratifiquen las operaciones que se ejecutan. Por tanto, las transacciones se incorporan a un nodo y posteriormente se difunden al resto de nodos que se encuentren en la red, que deberán de confirmar la operación.

Esto supone, básicamente, que el control no es de una única persona, sino que reside en todos los nodos del sistema, que, además, se encuentran en el mismo nivel y no por encima o por debajo de otro siendo necesaria la confirmación de todos los nodos de la red para asegurar la aceptación de una operación.

Resulta evidente que cuantos más nodos tenga el sistema, más complejo será para el delincuente o agente externo alterar la cadena de bloque o las transacciones, puesto que tan pronto como se altere la cadena de bloques de un nodo, esta será desestimada por el resto de nodos. El sistema realiza las verificaciones a través de funciones resumen o funciones hash como comentamos en el punto anterior.

Resumiendo, a medida que aumenta la descentralización, menos posibilidad existe de alterar las operaciones efectuadas.

- **Anonimato**

El anonimato es también una de las principales y más controvertidas características de las criptomonedas, ya que está muy relacionada con las actividades delictivas.

En primer lugar, se debe de diferenciar entre la privacidad y el anonimato. Mientras que la privacidad va ligada al desconocimiento del objeto de la transacción, pero no de sus actores, el anonimato va relacionado con a la identidad de las personas involucradas en la operación, tanto del remitente como del destinatario de una transacción.

Dentro del mundo de las criptomonedas resulta imposible saber la identidad de las personas, a diferencia de los bancos tradicionales donde las operaciones están vinculadas y no es posible realizar una transacción sin conocer la identidad de las personas implicadas.

La tecnología blockchain aporta confidencialidad al sistema, ya que el usuario no tiene que revelar su identidad para realizar transacciones, logrando de este modo proteger sus datos frente a terceros.

Aunque la cadena de bloques permite una cierta trazabilidad de las transacciones, si no se dispone de otros datos adicionales como, por ejemplo, la dirección IP del ordenador del usuario, su zona horaria, su geolocalización o la identificación del sujeto si ha recurrido a la vía ordinaria para convertir las criptomonedas en moneda de curso legal, el anonimato permanecerá. Hablamos pues de transacciones "pseudoanónimas" para la mayoría de tipos de moneda criptográfica, con la excepción de las creadas específicamente con características añadidas de anonimización.

¿Cómo se utilizan las criptomonedas?

A continuación, se mostrará, de una forma no técnica, cómo puede operar con criptomonedas cualquier usuario, específicamente con bitcoin al ser la criptomoneda más extendida.

Para poder recibir bitcoins, almacenarlos y utilizarlos hay que crear una billetera o monedero, que es esencialmente como cualquier otro monedero físico, incluso con varios compartimentos.

Ilustración 1. Billetera en papel

Un monedero o cliente, denominaciones utilizadas indistintamente, proporciona al usuario direcciones criptográficas, y contiene toda la información sobre el saldo, las transacciones y el historial del usuario siendo la interfaz con la red de bitcoin.

Conseguir un monedero es extremadamente sencillo y casi anónimo, ya que la mayoría de los proveedores de monederos no exigen ningún dato personal. Como un monedero no está vinculado al nombre de una persona física, proporciona anonimato. Se entiende pues que una persona puede tener varios monederos. Hay varios tipos de monederos de bitcoin: en entornos seguros en la nube o en un ordenador, incluso pueden tener forma física. Los describimos a continuación.

Billetera en papel

Monedero de papel (*paper wallet*) es la forma de nombrar las claves públicas y privadas impresas en un trozo de papel, como se muestra a continuación. Suele tener códigos QR que se pueden escanear rápidamente para añadir las claves a un monedero de software para realizar una transacción. Este tipo de monedero es más seguro que sus homólogos online, ya que se almacena físicamente y los hackers no pueden acceder a él. Sin embargo, como cualquier otro trozo de papel, puede romperse o sufrir daños elementales. Por lo tanto, la gente tiende a hacer múltiples copias físicas de este papel.

La ventaja de un monedero de papel es que las claves no se almacenan digitalmente en ningún sitio, por lo que no están sujetas a ciberataques o fallos de hardware. Varias webs en Internet ofrecen servicios de creación de monederos de papel para bitcoins.

Billetera hardware.

Los monederos de hardware son dispositivos independientes dedicados, que pueden contener claves privadas electrónicamente y facilitar los pagos. Suelen utilizar puertos USB y tienen que estar conectados al ordenador para realizar una transacción.

Ilustración 2. Billetera Hardware de "Ledger"

Los monederos hardware están protegidos del malware informático habitual porque generan las claves privadas fuera de línea, en el propio dispositivo. Son extremadamente seguros y, a la vez, cómodos de usar además de que no requieren la comprensión de complejos detalles técnicos.

Por otra parte, ofrecen sólidas opciones de copia de seguridad, para que los usuarios no pierdan el acceso a sus monederos. La mayoría de ellos están asegurados con un PIN y pueden incluir una protección adicional con contraseña para combatir los robos.

Billeteras software

Para poder utilizar las billeteras software deben ser descargadas e instaladas en el dispositivo electrónico que se vaya a utilizar, ya sea un ordenador, móvil, etc.

Su singularidad radica en que el usuario es el poseedor de las claves privadas (o de la semilla) para tener acceso a la gestión de fondos. Este sistema permite la posibilidad de acceder en off line lo que dificulta un posible hackeo.

Ilustración 3. Distintas marcas de billeteras software

Billeteras online

Los diferentes intercambiadores de criptomonedas, conocidos comúnmente como *Exchange,* proporcionan también aplicaciones y servicios para adquirir, gestionar y enviar criptomonedas en nuestra cuenta de usuario. A través de estas plataformas digitales se puede intercambiar criptomonedas por dinero FIAT. Son las más usadas en el mundo "cripto".

Resaltar que, en este sistema, las claves privadas están en manos de terceras partes: los *exchanges*, que las custodian para sus clientes. Estas billeteras son las más utilizadas por el usuario básico debido a la facilidad para la recepción, intercambio y uso de criptomonedas.

BINANCE COINBASE KRAKEN

Ilustración 4. Exchange

Obtención de criptomoneda

Actualmente se pueden obtener criptomonedas de manera muy sencilla. A continuación, se procede a describir los métodos más utilizados.

Intercambiadores de criptomonedas (*Exchange*)

La forma más fácil de obtener bitcoins es utilizar los intercambiadores o *exchange*[10] que funcionan como cualquier otro intercambio de divisas. Una vez registrado, el cliente puede convertir cualquier moneda en bitcoin. Hay cientos de bolsas disponibles como las que se muestran en la siguiente imagen.

Ilustración 5. Distintos logotipos de operadores exchange

10 . Un exchange de criptomonedas anidado proporciona a sus clientes servicios de trading de criptomonedas a través de una cuenta en otro Exchange.

Para utilizar un *exchange*, el cliente debe abrir una cuenta en línea con el intercambiador elegido. Aunque una clara mayoría de los intercambios populares requieren identificación y verificación para este propósito, algunos podrían alinear sus servicios hacia las necesidades de protección de sus clientes (criminales) y permitir la compra y venta sin requerir/exigir formas básicas de identificación y verificación de identidad (política de conocimiento del cliente; KYC acrónimo de *Know Your Customer).*

Ofrecen diferentes métodos de pago para comprar o vender monedas virtuales, principalmente, transferencias bancarias y pagos con tarjetas de crédito o débito. Algunos también ofrecen el uso de empresas de servicios monetarios, como Western Union y MoneyGram, PayPal, cheques bancarios e incluso dinero en efectivo, es decir, depósitos en efectivo, como dinero por correo. Las monedas virtuales también pueden cambiarse por otras monedas virtuales. Por ejemplo, algunos delincuentes convierten regularmente el bitcoin en Monero, otra criptodivisa que se acepta con menos frecuencia como método de pago en el mercado legal, pero presta un nivel de anonimato mayor.

A pesar de esto, la mayoría de los intercambiadores realizan su función en el lado legal del negocio y por tanto mediante solicitud podrían proporcionar información relativa a transacciones de las que conozcan pudiendo facilitar entre otros:

- *Copia de los documentos de identificación del cliente.*
- *Datos técnicos de comunicación: IP, número de teléfono, correo electrónico.*
- *Histórico de transacciones.*
- *Direcciones de depósito y retiro.*
- *Datos bancarios y transacciones a moneda FIAT.*

Intercambios P2P

También hay muchos vendedores en línea que venden bitcoin de forma privada a cambio de una pequeña comisión. Varios sitios en Internet ofrecen poner en contacto a personas que quieren intercambiarla cara a cara. *Localbitcoins.com* es uno de los principales mercados para personas dispuestas a comprar o vender bitcoin en persona. Algunos vendedores prefieren el pago en efectivo, mientras que otros permiten utilizar un servicio de pago en línea.

ATMs de criptodivisa

Ilustración 6. Cajero de criptomonedas

Estos cajeros automáticos permiten introducir dinero en efectivo a cambio de bitcoins, que se entregan en forma de recibo en papel o se transfieren a una dirección bitcoin.

Hay dos tipos diferentes de cajeros automáticos de bitcoin, los cajeros de solo compra de bitcoin y los cajeros de bitcoin que permiten la compra y venta de bitcoins, aunque predominan los cajeros de un solo uso.

La mayoría de los cajeros de bitcoin solo aceptan dinero en efectivo, ya que no están preparados para procesar transacciones con tarjetas de débito o crédito. Los cajeros automáticos de bitcoin permiten compras rápidas, ya que el comprador recibe bitcoins en su dirección casi al instante.

Muchos de ellos exigen un protocolo de KYC aunque otros siguen operando sin cumplir ninguna normativa existente de AML (*Anti- Money-Laundering*).

Para localizar los cajeros de criptomonedas se puede utilizar el sitio web: https://coinatmradar.com/.

Minería

La minería es un proceso por el que los nodos especializados en este tipo de gestión (mineros), procesan las transacciones de criptomoneda validando los bloques que se van generando resolviendo, mediante calculo computacional criptográfico, el hash -huella digital-agregando estos movimientos al libro de contabilidad distribuido. El minero recibirá por esta gestión nuevas criptomonedas generadas automáticamente por el sistema como recompensa.

La recompensa junto a las comisiones recibidas por la validación de cada una de las transacciones, es lo que incentiva a los mineros a ofrecer su potencial informático. Esta no es, evidentemente, una manera utilizada por el usuario medio para obtener criptomoneda.

El minado de criptomoneda no es una actividad ilegal en sí misma.

Ilustración 7. Minería de criptomonedas

Uso de las criptomonedas como facilitadores del blanqueo de capitales

El proceso tradicional del blanqueo de capitales comprende tres fases:

- **La colocación:** *del dinero ilegítimo en el sistema financiero legítimo.*
- **La estratificación: Separación de los fondos ilegítimos de su fuente mediante** *transacciones financieras que ofusquen su origen.*
- **Integración:** *Dar apariencia legítima mediante el reingreso en la economía con transacciones comerciales de apariencia legal.*

Por todo lo expuesto anteriormente, se pueden obtener criptomonedas de manera ágil y sencilla utilizando fondos de cualquier procedencia. Una vez adquiridas estas criptomonedas -colocación- y el ámbito del uso de estas para facilitar el blanqueo, existen varios factores que son determinantes, buscando principalmente perder la trazabilidad para su posterior monetización –estratificación e integración-.

Por tanto, a continuación, se va a detallar distintos actores que afectan a este proceso.

Trazabilidad y Monetización

"Nested services"

Estos servicios son una amplia categoría de servicios que operan dentro de una o más *exchange*. Utilizan las direcciones alojadas en los *exchange* para aprovechar la liquidez de las mismas y sacar provecho de las oportunidades de negociación. Algunos *exchange* no exigen normas estrictas de cumplimiento para los servicios anidados[11], lo que permite a los delincuentes explotarlos para el blanqueo de dinero.

En el libro mayor de la cadena de bloques, estas transacciones de servicios anidados aparecen como realizadas por sus contrapartes anfitrionas (es decir, las bolsas) en lugar de por los servicios anidados alojados o las direcciones de los individuos.

El tipo de servicio anidado más común y notorio es un corredor extrabursátil (OTC acrónimo de *Over the counter*: "bajo el mostrador").

Los corredores OTC permiten a los comerciantes negociar fácilmente, de forma segura y anónima, grandes cantidades de criptodivisas. Los *brokers* OTC facilitan las operaciones directas de criptodivisas entre dos partes, sin la mediación de un *exchange*. Estas operaciones pueden realizarse entre diferentes criptodivisas (por ejemplo, Ethereum y bitcoin) o entre criptodivisas y monedas fiduciarias (por ejemplo, criptodivisas, como bitcoin, y monedas fiduciarias, como euros o dólares). Los corredores OTC encuentran contrapartes para una transacción a cambio de una comisión, pero no se involucran en las negociaciones. Una vez definidos los términos, las partes transfieren la custodia de los activos a través del *broker*.

Plataformas de juego y apuestas

Las plataformas de juego son populares entre los blanqueadores de dinero en criptomonedas. Los fondos se ingresan en la plataforma a través de alguna combinación de cuentas identificables o anónimas. Se cobran o se colocan en apuestas, a menudo en connivencia con afiliados. Una vez que el dinero en la cuenta de juego se paga, se le puede dar un estatus legal. Los servicios de apuestas han sido especialmente señalados en el informe *"Virtual Assets Red Flag of Money Laundering and Terrorist Financing"* del Grupo de Acción Financiera Internacional (GAFI), publicado en septiembre de 2020.

En este informe, el GAFI identificó dos situaciones en las que los servicios de juegos de azar pueden ser considerados como una bandera roja:

- *Fondos depositados o retirados de una dirección o cartera de activos virtuales, con vínculos de exposición directa e indirecta a fuentes sospechosas conocidas, incluyendo sitios de juego cuestionables.*
- *Transacciones de VA originadas o destinadas a servicios de juego en línea.*

Mixers

Dado que las transacciones de bitcoin se registran y están disponibles públicamente a través de la cadena de bloques en Blockchain, estas no son totalmente anónimas y pueden ser rastreadas. Los servicios de mezcla (también llamados *tumblers*) se utilizan para mezclar los bitcoins de uno con los de otras personas con la intención de hacer más difícil reconstruir el historial de transacciones y rastrear la fuente original. Varios proveedores de servicios de mezcla ofrecen diferentes técnicas de mezcla a través de la web de superficie, pero también de la Darknet.

Exchange no confiables

Las *exchange* no confiables son los que no obedecen o no están sujetos a regulaciones o tienen programas de cumplimiento laxos. Estos *exchange* requieren poca o ninguna verificación de la identidad del usuario para transferir criptoactivos y, por tanto, son muy atractivas para los actores ilícitos.

11 . Un exchange de criptomonedas anidado proporciona a sus clientes servicios de trading de criptomonedas a través de una cuenta en otro Exchange.

Según un estudio reciente, el volumen de transacciones de los intercambios no conformes en 2020 ascendió a casi 20.000 millones de dólares, de los cuales 4.200 millones sirvieron para transacciones ilícitas, un aumento del 16% en el volumen de transacciones ilícitas en comparación con 2019. Esta investigación indica que los *exchange* no confiables son tan atractivos para los delincuentes que procesan 10 veces más transacciones ilícitas que las bolsas con políticas establecidas de CSC y Anti-lavado de Dinero (AML).

Servicios en paraísos jurisdiccionales

Los servicios con sede en jurisdicciones de alto riesgo son servicios en jurisdicciones identificadas con deficiencias estratégicas en sus regímenes de lucha contra el blanqueo de capitales o la financiación del terrorismo (CFT).

El Grupo de Acción Financiera Internacional (GAFI) identifica las jurisdicciones con medidas débiles de lucha contra el blanqueo de capitales y la financiación del terrorismo (ALD/CFT) en dos documentos públicos, que suelen denominarse externamente “lista negra” y “lista gris”. La Comisión Europea también identifica a los países que presentan deficiencias estratégicas en sus regímenes de PBC/FT y que suponen una amenaza significativa para el sistema financiero de la Unión Europea.

Criptomulas

Las “criptomulas” tienen el mismo funcionamiento que la utilización de mulas en el ámbito económico común. Estas son utilizadas en la creación de cuentas de un intermediario en los *exchange* para recepcionar los fondos y remitirlos a otro destino.

Compra entre particulares (comisionistas)

Estos comisionistas son personas físicas anunciadas en foros como en darkweb o conocidos a través de terceras personas, se encargan de poner en contacto a personas generalmente con un gran volumen de criptomonedas, mayormente bitcoins, con otros individuos que disponen de mucho dinero efectivo de procedencia ilícita. Por este servicio suelen cobrar entre el 1-5 % del valor de la transacción.

Darkmarket

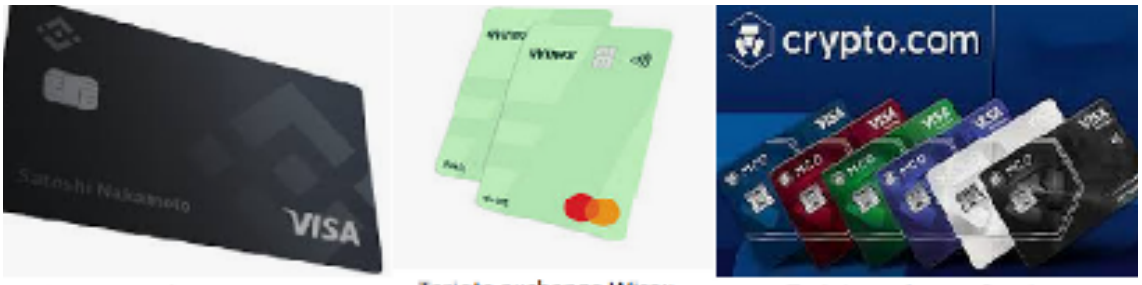
Los darkmarkets (mercados negros) son mercados ubicados en la llamada darkweb donde no se puede acceder con navegadores convencionales. Estos mercados operan con criptomonedas, al realizar envíos y retiradas en los distintos mercados la trazabilidad de los fondos se pierde, ya que todos son almacenados en un pool común.

Tarjetas de criptomonedas

Las tarjetas tradicionales suelen estar vinculadas a una cuenta bancaria, mientras las tarjetas de criptomonedas permiten al usuario acceder a la capacidad adquisitiva de sus criptomonedas. La mayoría de estas tarjetas son proporcionadas como un servicio adicional en la cuenta de muchos *exchange*.

La mayoría de estas requieren un protocolo de identificación para uso, el uso de estas está muy extendido, ofrece capacidades de pago en establecimientos en TPV, así como la disponibilidad de efectivo en los cajeros, lo que hace muy atractivo su uso por su accesibilidad y rapidez.

Ilustración 8. Tarjetas de criptomonedas



Tarjeta exchange Binance | Tarjeta exchange Wirex | Tarjeta exchange Crypto.com

Exchanges descentralizados

Los *exchanges* descentralizados, conocidos como DEX, son plataformas en las que se realizan acciones y venta de criptoactivos. La principal diferencia es que el funcionamiento interno de la plataforma se ejecuta directamente en la blockchain mediante Smart contracts, piezas de código que eliminan intermediarios regidos por un protocolo. Sus ventajas son amplias desde anonimato, seguridad, bajas comisiones.

Criptomonedas privadas

Las criptomonedas privadas por las características de su protocolo hacen imposible la trazabilidad de transacciones en su blockchain, por lo que son muy usadas si se busca la privacidad y opacidad. Las más conocidas son Monero, ZCash, Dash, Verge, Komod.

Investigación. Redes de cooperación y unidades especializadas

Las investigaciones dentro del ecosistema virtual de la criptomoneda pueden ser altamente complejas. Sin embargo, suponen la aparición de una nueva vía de seguimiento y vigilancia para cualquier tipo de actividad criminal incluida la del lavado de capitales.

Para ello resultan determinantes varios factores: la cooperación policial y judicial internacional, la potenciación de la colaboración con el sector privado, y la formación de estructuras policiales especializadas.

En cuanto a la **cooperación internacional**, policial en este caso, decir que resulta necesario el disponer de un espacio común de intercambio de información operativa tanto a nivel bilateral como contando con estructuras supranacionales. Este es el marco adecuado también para la homogenización de formación, procedimientos, técnicas y buenas prácticas. Por último, en estas organizaciones se pueden concentrar los medios humanos y técnicos especializados que den soporte a los países que lo necesiten.

La **colaboración con el sector privado** es fundamental. Se han enumerado en esta guía muchos de los actores que intervienen en el mundo cripto. Muchos de ellos son entidades dispuestas a colaborar con las fuerzas del orden o la autoridad judicial en su caso, por lo que resulta interesante el establecimiento de los canales adecuados de comunicación con estas. Las sinergias entre la investigación técnica policial y la colaboración de las entidades privadas son la clave en el éxito.

La **investigación tecnológica,** en general, representa un reto para todas las organizaciones encargadas del mantenimiento de la ley.

Exige de estas una adaptación en cuanto estructuras, debiendo generar o modificar aquellas que dentro de su organización estén en mejor disposición de abordar esta especialidad. La creación de Unidades especializadas en el nuevo entorno virtual es algo imprescindible para un cuerpo policial actualizado a la realidad de nuestra sociedad.

La **selección y formación de personal** es una de las piezas claves en este proceso de adaptación. Se ha de procurar establecer un programa de formación modular, progresivo y multidisciplinar, procurando la continuidad del personal especializado como forma de retención del talento. En este programa de formación tecnológica una de las nuevas materias es el análisis y trazabilidad de criptomoneda incluyendo investigación en fuentes abiertas especializada.

Esta función debe llevarse a cabo por personal **altamente especializado y con dedicación exclusiva**. La necesidad de la investigación de la criptomoneda es transversal a todo tipo de criminalidad, por lo que este equipo de especialistas cripto pueden dar soporte a los investigadores principales de cualquier modalidad delictiva.

Otro de los aspectos importantes a tener en cuenta son los **medios necesarios** para llevar a cabo

esta labor. Las herramientas especializadas en la investigación y trazabilidad de criptomoneda suponen una importante inversión económica, por lo cual hay que valorar bien su despliegue. No se debe tampoco abandonar la filosofía de “navaja suiza” utilizada en otros ámbitos de investigación tecnológica, es decir el contar con un set de “herramientas” que permitan la verificación de las hipótesis de investigación. En este punto, hay que insistir de nuevo, en que la formación especializada y certificada en las herramientas que se utilicen es determinante.

CONCLUSIONES

La tecnología que soporta las distintas criptomonedas se ha asentado rápidamente en nuestra sociedad. Los criminales hacen uso de cualquier herramienta a su alcance para llevara a cabo sus actividades y esta no es una excepción. El aprovechamiento de las ventajas que proporciona la criptomoneda: seguridad, anonimato, y rapidez en un entorno global no fiscalizado, ha sido rápidamente adoptado por delincuentes de todo tipo.

Sin embargo, existen nuevas formas de investigación adaptadas a esta nueva circunstancia, que proporcionan una nueva vía de obtención de información en la resolución de todo tipo de criminalidad y especialmente en el uso de la criptomoneda en el lavado de capitales.

Para ello las distintas instituciones deben adaptarse rápidamente a esta circunstancia, por un lado, favoreciendo e impulsando la cooperación internacional judicial y policial, dotando de una normativa homogénea y eficaz al conjunto de la comunidad y proporcionando mecanismos de investigación reales y efectivos.

En este sentido, es importante contar con profesionales formados en esta tecnología, tanto en el ámbito judicial como en el de experto investigador policial. Estos profesionales deben contar con las estructuras y medios adecuados para cumplir con su deber de forma adecuada.

RECOMENDACIONES DE ACTUACIÓN FUTURA

- **Generación y armonización de un marco jurídico adecuado.**

  Se deben acometer los cambios legales necesarios para incluir el fenómeno de los criptoactivos en el marco jurídico teniendo como objetivo la prevención del lavado de activos.

- **Facilitar la cooperación judicial y policial entre los Estados.**

  Se precisan instituciones y mecanismos que proporcionen un marco adecuado no solo para el intercambio de información desde el punto de vista operativo, si no también para prestación de servicios especializados, formación y coordinación de equipos conjuntos de investigación, armonización de la formación y formulación de metodologías y buenas prácticas.

- **Establecimiento de unidades especializadas en investigación tecnológica y económica.**

  Desde el punto de vista policial se debe considerar las amenazas procedentes del mundo virtual y tecnológico. La manera más eficaz de luchar contra estas amenazas consiste en el establecimiento de Unidades con personal especializado, haciendo hincapié en el diseño de un plan de formación modular y progresivo, así como de la dotación de medios técnicos adecuados.

- **Formación específica para tribunales y fiscales especializados.**

  Los cambios en esta sociedad altamente globalizada y tecnológica son vertiginosos. La aparición de novedades tecnológicas tiene por consecuencia adaptaciones prácticamente inmediatas del mundo del crimen para su uso ilegítimo. Entender dichos cambios y sus implicaciones legales resulta fundamental, debiéndose fomentar la actualización de conocimientos en este sentido.

BIBLIOGRAFÍA

Página oficial de la Fiscalía General del Estado de España (2021).

www.fiscal.es

Legislación consolidada en el BOE (búsqueda) (2021).

http://www.boe.es/legislacion

SEPBLAC (2021).

http://www.sepblac.es

Guías de buenas prácticas. Lucha contra el tráfico de drogas. Asociación· Ibero Americana de Ministerios Públicos (AIAMP) (2013).

Base de datos Lotus Notes-Jurisprudencia del Tribunal Supremo español (2021).

Legislación europea-Eurlex (desde el BOE español) (2021).

Base de datos El derecho.com (2021).

INTERPOL Directrices sobre la red oscura y la criptomoneda. Guía para profesionales (2020).

INTERPOL 5th Interpol Working Group on Dark Web and Virtual Assets (2021).

EUROPOL. IOCTA Internet organised crime treat assessment (2021).

EUROPOL. A guide for bitcoin Investigators (2016).

Consejo Europa – iPROCEEDS-2. Guide on Seizing Cryptocurrencies (2021).

Chainalysis. The 2020 State of Crypto Crime (2021).

Chainalysis. Cryptocurrency fundamentals (2021).

Insigth2- OLAF. Financial Tech Open Source Intelligence (2021).

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

EL PAcCTO es un programa de cooperación internacional financiado por la Unión Europea que persigue promover la seguridad ciudadana y el Estado de derecho en América Latina a través de una lucha más efectiva contra el crimen transnacional organizado y de una cooperación fortalecida en la materia. Cubre los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela. Es la primera vez que un programa regional europeo trabaja en toda la cadena penal para fortalecer la cooperación a través de tres componentes (cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios) con cinco ejes transversales (cibercrimen, corrupción, derechos humanos, género y lavado de activos).

Programa liderado por

FIIAPP COOPERACIÓN ESPAÑOLA

EXPERTISE FRANCE

Socios coordinadores

iila

CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL

PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA