REVISTA 3.9 APM

JOAQUÍN DELGADO MARTÍN

AUDIENCIA NACIONAL

INVESTIGACION E INCAUTACIÓN DE LAS CRIPTOMONEDAS

1.- Introducción

1.1.- Criptomonedas en el delito

1.2.- Activos Virtuales

1.3.- Proveedores de Servicios de Activos Virtuales

1.4.- Retos de la investigación

2.- Obtención de datos para la persecución de delitos

2.1.- Análisis blockchain

2.2.- Solicitud de información (datos) a los proveedores de servicios de activos virtuales (PSAV)

2.3.- Otras medidas de investigación tradicionales

3.- Incautación (aprehensión) de criptoactivos

3.1.- Criptoactivos en monederos custodiados por proveedores (hosted wallets).

3.2.- Criptoactivos en monederos no custodiados por proveedores (unhosted wallets)

1.- Introducción

1.1.- Criptomonedas en el delito

Las criptomonedas se han convertido en un instrumento relevante para la delincuencia, debido a características como el pseudonimato, la descentralización y la facilidad para

realizar transacciones transfronterizas. En este contexto, pueden identificarse tres grandes ámbitos de utilización ilícita.

En primer lugar, **como medio de pago de servicios criminales**. Estas transacciones suelen tener lugar en entornos ocultos de Internet, como la *dark web* o Internet profunda, donde se facilita la compraventa de bienes y servicios ilegales. Entre ellos se incluyen estupefacientes, moneda falsificada, documentos de identidad falsos, datos de tarjetas bancarias robadas o clonadas, software malicioso (*malware*), material de explotación sexual infantil, así como armas y explosivos. El uso de criptomonedas en estos mercados permite a los intervinientes reducir su exposición y dificultar la trazabilidad de las operaciones.

En segundo lugar, las monedas virtuales pueden emplearse como **instrumento para la comisión de fraudes**. En el ámbito privado, esto se traduce en estafas dirigidas a particulares mediante múltiples modalidades. En el ámbito público, su utilización puede vincularse a delitos fiscales, especialmente en relación con la ocultación de rendimientos económicos obtenidos a través de operaciones con criptoactivos.

Finalmente, las criptomonedas desempeñan un papel relevante en el **blanqueo de capitales** de origen ilícito, proceso que suele estructurarse en tres fases. En la fase de colocación, el dinero procedente de actividades delictivas se convierte en moneda virtual, transfiriéndose desde el sistema financiero tradicional a plataformas de intercambio para adquirir criptoactivos como Bitcoin o Ethereum. En la fase de estratificación, se llevan a cabo múltiples operaciones destinadas a dificultar la trazabilidad de los fondos, como el uso de mezcladores o el intercambio entre diferentes criptomonedas que ofrecen mayores niveles de privacidad (*chain hopping*). Por último, en la fase de integración, los fondos se reintroducen en la economía legal mediante su conversión en otros activos o en dinero fiduciario, permitiendo así la aparente legitimación de las ganancias ilícitas

1.2.- Activos Virtuales

El término de activos virtuales (AV) no es un concepto homogéneo, sino que se trata de un término paraguas para describir una serie de tokens que presentan una amplia gama de características. De esta manera, no existe uniformidad en la terminología utilizada para referirse a los AV: entre los términos utilizados están criptomonedas, monedas virtuales, activos digitales, entre otros. (para más información se puede consultar el Anexo respectivo)[1].

Buscando un concepto que pueda ser reconocido por los distintos Estados, acudimos a la definición de GAFI: "un activo virtual es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los activos virtuales no incluyen representaciones digitales de moneda fiat, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI"[2]. Como vemos, GAFI busca abarcar la gama más amplia de instrumentos virtuales

[1] "Guía para la Regulación ALA/CFT de Activos Virtuales y Proveedores de Servicios de Activos Virtuales en la Región del GAFILAT"

[2] GAFI (2012-2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, página 140

que pueden utilizarse con fines de lavado de activos y financiación de terrorismo. De acuerdo con el Glosario de GAFI.

> **Activo Virtual**
>
> Es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones

En la normativa española, cabe destacar el artículo 1.5 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, según el cual "*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"*.

1.3.- Proveedores de Servicios de Activos Virtuales

Según el Glosario GAFI[3], "proveedor de servicios de activos virtuales" (PSAV) es "cualquier persona física o jurídica que no esté cubierta en ningún otro lugar en virtud de las Recomendaciones y que, como negocio, realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica: i) intercambio entre activos virtuales y monedas fiat; ii) intercambio entre una o más formas de activos virtuales; iii) transferencia de activos virtuales; iv) custodia y / o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales; y v) participación y provisión de servicios financieros relacionados con la oferta de un emisor y / o venta de un activo virtual."

Como puede observarse, los países deben adoptar un **enfoque funcional** para determinar si las operaciones y actividades de una persona natural o jurídica son las de un PSAV[4]. Se puede realizar la clasificación que se contiene en el siguiente cuadro:

[3] GAFI (2012-2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, página 140

[4] "Los países no deben aplicar su definición basándose en la nomenclatura o la terminología que la entidad adopta para describirse a sí misma o en la tecnología que emplea para sus actividades. Como se ha indicado anteriormente, las definiciones no dependen de la tecnología empleada por el proveedor de servicios. Las obligaciones en los Estándares del GAFI se derivan de los servicios financieros subyacentes ofrecidos sin tener en cuenta el modelo operativo de una entidad, las herramientas tecnológicas, el diseño del libro mayor o cualquier otra característica operativa" (GAFI, "Guía actualizada para un enfoque basado en el riesgo a los activos virtuales y proveedores de servicios de activos virtuales,", 2021, página 23)

PSAV dentro de las Recomendaciones del GAFI	Servicios de cambio de AV, monederos de AV, intermediación en AV, proveedores de ofertas iniciales de monedas (ICO), proveedores de plataformas de negociación de AV, proveedores de gestión de AV.
PSAV fuera de las Recomendaciones del GAFI	Validadores/mineros, operadores de red, host de nodos, servicios de información, servicios de alojamiento, autoridad de certificación, mezcladores, servicios de administración web, exploradores blockchain, emisores de moneda.

1.4.- Retos de la investigación

La investigación de delitos relacionados con criptoactivos se ha de enfrentar a dos retos principales:

1º.- La **obtención de información (datos)** relevantes para la persecución penal, con dos objetivos principales: a) identificar y localizar los criptoactivos; y b) recopilar pruebas que relaciones los criptoactivos con los delitos investigados y/o con las personas responsables

2º.- Una vez identificados, el sistema penal ha de enfrentarse al desafío de la **aprehensión (incautación) de los criptoactivos**, no solamente para la reparación de las víctimas, sino también para ejecutar el decomiso y para atender a otras responsabilidades pecuniarias (multas)

Ambos retos presentan una **dimensión internacional** que dificulta su investigación y enjuiciamiento, y que ha de ser necesariamente afrontada para incrementar la efectividad de la persecución de los delitos

2.- Obtención de datos para la persecución de delitos

La presencia de criptoactivos aporta elementos de complejidad a la investigación, pero ésta es posible mediante una combinación de medidas de investigación de diferente naturaleza:

2.1.- Análisis blockchain

Una vez conocida una dirección pública de criptomoneda (que puede haber sido obtenida por otros medios de investigación contemplados en otros puntos del presente apartado), la naturaleza descentralizada y pública de las blockchains permite la utilización de herramientas de análisis de las cadenas de bloques.

Una transacción criptográfica en un libro mayor de blockchain es identificable inicialmente por una dirección pública (transparencia del libro mayor). Como quiera que los datos de las blockchains son de acceso público, el acceso a los mismos tiene la consideración de

fuentes abiertas, a las que se puede acceder desde cualquier país al amparo de lo dispuesto por el artículo 32 del Convenio de Budapest.

Sin embargo, los exploradores de bloques no identifican a las personas y entidades de las transacciones, por lo que son necesarios otros instrumentos para analizar las transacciones de criptomonedas; identificar las contrapartes implicadas y con identidades del mundo real; y descubrir relaciones ocultas y patrones. A tal efecto pueden aplicarse instrumentos de **inteligencia en fuentes abiertas u OSINT** (Open Source Intelligence).

Por un lado, se pueden utilizar **motores de búsqueda especializados**[5] con los que, tras insertar la dirección pública de una wallet, se puede recopilar información que puede ser relevante pero limitada: constatar si esa dirección ha sido ya usada; si contiene activos, la naturaleza y el importe de estos activos; entre otros datos.

Por otro lado, los investigadores también pueden usar **herramientas de análisis blockchain**[6]. Sobre la base de los datos de acceso público de las cadenas de bloques (junto con otros datos que aportan los propios investigadores obtenidos por otros medios legítimos de investigación), utilizan algoritmos para construir informaciones que permiten avanzar en el conocimiento del trazado de los criptoactivos y sus relaciones. En una primera fase, mediante la agrupación (Clustering) de tal manera que simplifica el libro mayor, y se asocian las direcciones utilizadas por la misma persona o entidad. En una segunda fase de identificación, se asocian las direcciones a las entidades (PSAV): recopilación de datos haciendo depósitos reales; expertos identifican las direcciones de los servicios; y se realiza el reconocimiento y análisis de patrones para identificar (vincular) direcciones a servicios específicos. Y una tercera fase de visualización, que muestra el flujo de transacciones entre los grupos de direcciones analizados

Tras la utilización de las anteriores herramientas de análisis blockchain, se llega al PSAV: se abre paso la siguiente modalidad de investigación, esto es, la solicitud de información al proveedor de servicios

2.2.- Solicitud de información (datos) a los proveedores de servicios de activos virtuales (PSAV)

Los titulares de wallets de criptomonedas realizan operaciones con ellas: adquieren bienes y servicios; cambian criptomonedas por moneda fiat, especialmente dólares y euros; cambian unas criptomonedas por otras; alojan las criptomonedas en carteras alojadas (hosted wallet).... Como quiera que estas operaciones se realizan con la intervención de proveedores de servicios de activos virtuales (PSAV), estos proveedores disponen de datos que pueden resultar muy útiles en las investigaciones de delitos

Estos proveedores pueden aportar, en primer lugar, los datos que ha utilizado un cliente para identificarse ante el PSAV (*Know Your Customer* - KYC): documento de identidad oficial, identificación biométrica, verificación por un tercero...Asimismo, cada tipo de PSAV puede aportar otros datos directamente relacionados con los servicios que ofrecen a sus clientes: los "exchanges" que permiten negociar criptoactivos, intercambiarlos por moneda fiduciaria y acceder a otros servicios financieros; local traders que permiten

[5] Por ejemplo, blockchain.info, etherscan.io o blockchaintrail.com

[6] Estos productos son utilizados para investigaciones internas (compliance) y para investigaciones públicas (Policía, reguladores, autoridades financieras): TRM, Ciphertrace, Chainalysis (Reactor)

realizar transacciones *peer-to-peer*, intercambiando directamente criptomonedas con personas dispuestas a entregar moneda fiduciaria; procesadores de pagos de moneda virtual, que facilitan la transferencia de pagos de moneda virtual de un usuario (cliente) a un comerciante o a otros negocios o profesional que ofrece bienes o servicios de consumo; entre otros.

Las vías de acceso a estos datos en poder de PSAV son básicamente dos: la solicitud directa al proveedor con fundamento en el principio de voluntariedad, remitido especialmente mediante vías de cooperación policial internacional; y la solicitud de cooperación judicial internacional con fundamento en un convenio, o bien mediante la emisión de la Orden Europea de Investigación si el PSAV se encuentra en otro país de la UE.

Cuando se utiliza la solicitud directa, es necesario tener en cuenta de forma especial dos precauciones: comprobar previamente si el PSAV requerido es fiable (posible implicación en actividades delictivas); si coopera con los investigadores del sistema penal y cómo lo hace; y qué régimen de confidencialidad aplica, porque concurre el riesgo de que informe a su cliente de la solicitud de información recibida aplicando su normativa interna[7].

2.3.- Otras medidas de investigación tradicionales

Otras medidas de investigación tradicionales (allanamientos, vigilancias, cacheos...) y tecnológicas (registro de dispositivos, interceptación de comunicaciones...) pueden resultar de utilidad para llegar a conocer la existencia de **billeteras**[8] y **claves**, que se pueden encontrar en múltiples formas. Por ejemplo, se puede encontrar una dirección escrita en una hoja de papel, en un recibo de cajero automático de criptomonedas o en el dispositivo electrónico (ordenados, teléfono móvil, tablet...) de un sospechoso, ubicada en notas, mensajes de texto, mensajes de aplicaciones o incluso fotos. Asimismo, es probable que la información más confidencial (las claves privadas) se oculte en un formato más seguro: en una hoja de papel almacenada en un lugar seguro; o escondida dentro de una aplicación móvil.

Asimismo, estas otras medidas de investigación pueden permitir el conocimiento de **frases semilla**, es decir, una serie de palabras aleatorias (frases semilla) que son generadas por una billetera de criptomonedas. Suelen tener 12, 24 o 25 palabras. Con las mismas se asegura el acceso a los fondos en esa billetera (acceso, respaldo o recuperación), tratándose de una versión legible de una clave privada. Estas palabras pueden escribirse en papel, almacenarse en un archivo en un dispositivo o incluso imprimirse en metal para protegerlas de los daños causados por el fuego.

Con estas medidas también se pueden obtener **recibos de cajeros automáticos** de critpomonedas (crypto ATMs), que pueden ser recibos en papel de un cajero automático tradicional o recibos digitales enviados por mensaje de texto o correo electrónico.

[7] Constituye una buena práctica que la solicitud de información al PSAV se señale expresamente que debe posponer la comunicación al cliente sobre la cesión de sus datos a las autoridades públicas durante un determinado período

[8] La billetera o cartera cuenta con un software que permite la comunicación con la red, que genera y almacena claves privadas; y la clave privada genera una dirección para enviar fondos (o para desbloquear los fondos recibidos para permitir su reenvío)

Contienen la fecha de la transacción, la cantidad de criptomonedas y monedas compradas y la dirección de depósito. Los formatos y detalles específicos varían de un cajero automático a otro. Y también pueden ser relevantes los datos sobre **consumos eléctricos**, porque los mineros de criptomonedas son computadoras que crean criptomonedas y pueden consumir cantidades significativas de electricidad.

Por último, cabe hacer una referencia a que este tipo de medidas de investigación pueden permitir la localización de carteras de hardware ("almacenamiento en frío" - **Cold Wallets**). Se trata de billeteras no conectadas a internet que se utilizan para almacenar criptomonedas, y que se encuentran en soportes físicos a los que se accede mediante una clave. Tienen capacidad para enviar y recibir criptodivisas al conectar al dispositivo habilitado para Internet y bajo autorización, y una vez finalizada la transacción desconectarlo de toda red. Resulta relevante tanto el registro de dispositivos, como el conocimiento de las claves de acceso que pueden obtenerse por las vías anteriormente mencionadas.

3.- Incautación (aprehensión) de criptoactivos

La persecución de la delincuencia ligada a las criptomonedas ha de enfrentarse al desafío de la incautación, que puede acordarse por la autoridad judicial competente de forma provisional (embargo) o de forma definitiva (decomiso). Cuenta con dos modalidades básicas atendiendo al tipo de cartera (wallet) afectado: alojadas y no alojadas.

3.1.- Criptoactivos en monederos custodiados por proveedores (hosted wallets).

En estos casos, las claves privadas son mantenidas por un tercero (por ejemplo, Coinbase, Binance, Gemini). La aprehensión tendrá lugar mediante el requerimiento a la empresa Exchange para la transferencia de los activos al Estado; en concreto mediante una billetera del Poder Público creada al efecto, o bien a una billetera gestionada por un PSAV que haya convenido con el Estado. Una vez realizada la transferencia, los criptoactivos afectados queda decomisado, es decir, se ha producido aprehensión definitiva del bien (pérdida de titularidad por delincuente y atribución al Estado).

Pues bien, este requerimiento de transferencia ha de ser realizado, previa orden de juez competente según Derecho interno, mediante una solicitud de cooperación jurídica internacional (MLA) al amparo del convenio internacional que resulte aplicable: Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas), Convención de Palermo contra la Delincuencia Organizada Transnacional, Convención de Naciones Unidas contra la Corrupción, entre otros.

Las autoridades del sistema penal pueden remitir una solicitud de congelación de los criptoactivos afectados directamente al proveedor, y éste podrá atenderla de forma voluntaria de conformidad con su normativa interna.

Una vez realizada la transferencia, se aplica el Derecho nacional del Estado que acordó la aprehensión para resolver las siguientes cuestiones: ¿qué tipo de resolución judicial ha de ser adoptada? ¿cómo documentar la transferencia? ¿cómo se custodian los criptoactivos transferidos? ¿cómo respetar las garantías procesales del titular de los criptoactivos?.... Y dicho Derecho interno deberá decidir qué hacer con los criptoactivos: mantenerlos, cambiarlos por otras criptomonedas, o bien proceder a su cambio por moneda fiat. Teniendo en cuenta el gran riesgo de fluctuación de las criptomonedas, el Derecho

nacional puede otorgar la consideración de bienes perecederos o volátiles, procediendo de esta manera a su realización anticipada: cambio por moneda fiat de manera provisional antes de la finalización del proceso mediante resolución firme de decomiso. Lo óptimo consiste en que el ordenamiento nacional regule estas cuestiones de forma suficiente.

Una de las principales cuestiones a tener en cuenta es la gestión de la clave privada y de la fase semilla que permiten acceder a la cartera: se han de establecer los procedimientos adecuados para evitar riesgos en su gestión. Una buena práctica puede consistir en anotar la frase semilla dividida en varias partes, distribuyendo cada parte entre varias personas; así como en registrar la clave privada de forma similar, en al menos tres documentos diferentes, y almacenarlos en ubicaciones separadas y seguras

3.2.- Criptoactivos en monederos no custodiados por proveedores (unhosted wallets)

En estos supuestos, el usuario mantiene el control de las claves privadas (por ejemplo, Trust Wallet, Electrum, Exodus). La tenencia de la billetera o cartera está ligada a la posesión de la clave privada; no basta con estar en posesión de la billetera. Si se conoce la clave privada, se podrá proceder a su "realización" en los mismos términos que se han expuesto para las carteras custodiadas. Y, por otro lado, se podrá requerir a la persona condenada para que indique la clave privada, poniéndola a disposición de la autoridad pública.