Programa de Cooperación entre América Latina, el Caribe y la Unión Europea en Políticas sobre Drogas

Financiado por la Unión Europea

COPOLAD

CFATF GAFIC

Investigaciones financieras y análisis para riesgos emergentes de blanqueo de capitales:

Uso delictivo de criptomonedas

Investigaciones financieras y análisis para riesgos emergentes de blanqueo de capitales:

Uso delictivo de criptomonedas

Secretaría del GAFIC

Desde febrero hasta marzo de 2024, el Grupo de Acción Financiera Internacional del Caribe (GAFIC) y el programa COPOLAD III colaboraron para impartir una serie de talleres de formación impactantes sobre investigaciones y análisis financieros sobre riesgos emergentes de blanqueo de capitales. Estos talleres proporcionaron a investigadores financieros, analistas y otros actores de toda la región conocimientos y herramientas fundamentales para abordar los retos cambiantes del blanqueo de capitales, en particular, el uso indebido de activos virtuales. Basándose en la experiencia compartida durante estas sesiones, COPOLAD III ha desarrollado este completo manual de formación, que ha sido aprobado formalmente por los jefes de las unidades de información financiera (UIF) del GAFIC. Este manual constituye un recurso vital para mejorar la capacidad de la región en la lucha contra el blanqueo de capitales, dotando a los profesionales de los conocimientos y estrategias necesarios para explorar las complejidades del panorama de la delincuencia financiera.

COPOLAD III es un consorcio formado por:

Socios colaboradores.

[logo: FIIAPP COOPERACIÓN ESPAÑOLA]	[logo: iila Organizzazione internazionale italo-latino americana]	[logo: EUDA AGENCIA DE LA UNIÓN EUROPEA SOBRE DROGAS]	[logo: Sociedad Alemana para la Cooperación Internacional (GIZ)

COPOLAD III es un programa financiado por la Unión Europea y forma parte de la creciente cooperación entre la UE y los países de América Latina y el Caribe en el ámbito de la lucha contra el tráfico de drogas. La IILA[1] forma parte del Consorcio que gestiona el Programa, junto con la agencia española FIIAPP, el Observatorio Europeo de las Drogas y las Toxicomanías (EMCDDA, por sus siglas en inglés) y la Sociedad Alemana para la Cooperación (GIZ).

El objetivo del Programa es contribuir a la reducción de la demanda y la oferta de drogas en los países de ALC facilitando la generación y aplicación de políticas de lucha antidroga más equilibradas, basadas en la evidencia, integrales y, por tanto, más eficaces, respetando plenamente la soberanía nacional de los países de ALC de acuerdo con el principio de no injerencia en los asuntos internos de los Estados.

El Grupo de Acción Financiera del Caribe (GAFIC), la agencia española FIIAPP y la IILA han firmado un memorando de entendimiento cuyos principales objetivos son:

1. **Fortalecer** el intercambio de información entre ALC y los países europeos en el marco de las investigaciones financieras y patrimoniales vinculadas a delitos de tráfico de drogas.

2. **Mejorar** las capacidades de los analistas y funcionarios públicos a cargo de las investigaciones relacionadas con el blanqueo de capitales.

3. **Apoyar** la adopción, por parte de los países miembros del GAFIC, de normas, procedimientos y reglamentos que fortalezcan la capacidad de investigación de los delitos de blanqueo de capitales y la identificación y recuperación de activos procedentes del tráfico internacional de drogas.

1. La Organización Internacional Italo-Latinoamericana (IILA) es una organización intergubernamental con sede en Roma, cuyos miembros son: Argentina, Bolivia, Brasil, Colombia, Costa Rica, Cuba, Chile, Ecuador, El Salvador, Guatemala, Haití, Honduras, Italia, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. Desde su creación, la IILA ha desempeñado un papel importante en la facilitación de las relaciones entre Italia, Europa y América Latina, acción que se lleva a cabo operando en el ámbito cultural, socioeconómico, técnico-científico y de cooperación, mediante el uso de herramientas como: reuniones con especialistas del sector, patrocinio de eventos y becas, promoción de congresos, conferencias, exposiciones y otros eventos, y ejecución de proyectos de cooperación en los países latinoamericanos.

Este manual constituye un resumen de los temas clave derivados del curso sobre "Investigaciones y análisis financieros para riesgos emergentes de blanqueo de capitales" impartido en línea entre el 29 de enero y el 7 de marzo de 2024.
La información y los dictámenes formulados en este manual no reflejan necesariamente el dictamen oficial de la Comisión Europea. Ni la Comisión Europea ni ninguna persona que actúe en su nombre son responsables del uso que pueda hacerse de la siguiente información.

En el curso intervinieron los siguientes ponentes::

Miguel SMALDONE
Maresciallo Maggiore de los Carabinieri (Italia)

Ricardo Jorge DAVID
Agente de la Polícia Judiciária, Portugal

RJ BERRY
Director de la Autoridad de Información Financiera de las Islas Caimán

Federico PAESANO
Experto en activos virtuales (Italia)

Kisha SUTHERLAND
Directora de la Unidad de Recuperación de Activos del Sistema de Seguridad Regional (RSS ARU, por sus siglas en inglés)

Mirko LAPI
Consultor experto en OSINT

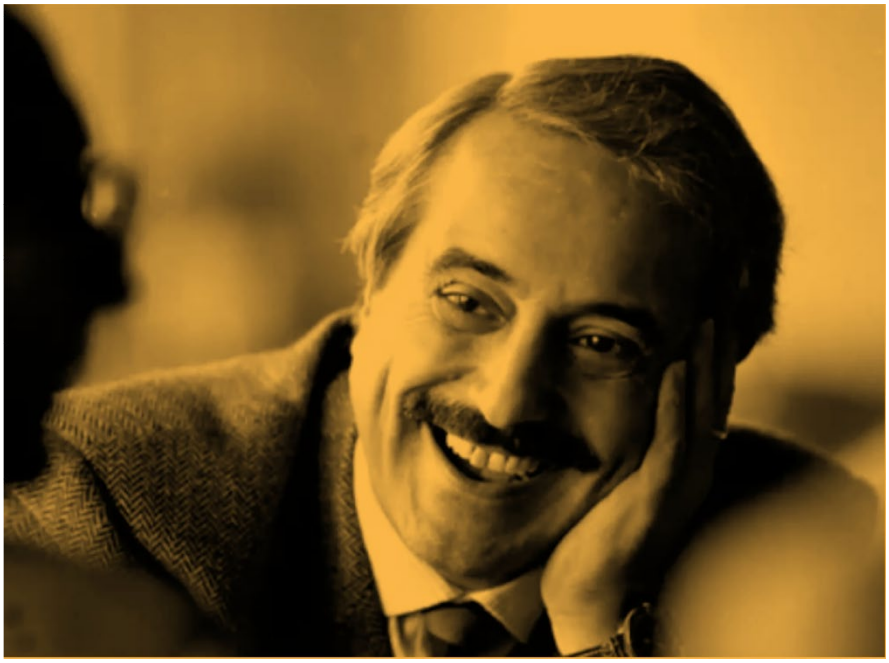
Contenido

1. Introducción

Giovanni Falcone, magistrado italiano, dedicó su vida a la lucha contra la delincuencia organizada y fue uno de los primeros defensores de la colaboración mundial en este cometido. Poco antes de su trágico asesinato, el 23 de mayo de 1992, participó en Viena en la sesión inaugural de la Comisión de Prevención del Delito y Justicia Penal, establecida por la Asamblea General de las Naciones Unidas. Esto marcó el inicio de una entidad de las Naciones Unidas con la misión específica de hacer frente a la delincuencia, sentando las bases para una mayor coordinación de los esfuerzos internacionales contra la delincuencia organizada.

Motivado por un excepcional sentido del deber, Falcone fue pionero en la aplicación de un innovador enfoque de investigación centrado en “seguir el dinero” en las pesquisas financieras relacionadas con bancos e instituciones financieras tanto en Italia como en el extranjero. Este método resultó decisivo para rastrear el movimiento de activos sospechosos y establecer sus conexiones con actividades delictivas organizadas. El legado del enfoque de Falcone perdura a nivel internacional para combatir la delincuencia organizada.

Seguir el dinero... ¡y las criptomonedas!



Esto se puede interpretar, hoy en día, como “seguir las criptomonedas”

En los últimos años, el panorama financiero ha sido testigo de un auge sin precedentes de los avances tecnológicos, concretamente en los métodos de pago electrónicos. Si bien estas innovaciones ofrecen comodidad, también plantean preocupaciones por el blanqueo de capitales y la financiación del terrorismo, ya que los delincuentes pueden explotar estos canales avanzados para actividades ilícitas. La tecnología evoluciona con rapidez, mientras que los marcos legislativos a menudo se quedan atrás, lo que crea una brecha que los delincuentes explotan fácilmente, especialmente en el ámbito del movimiento mundial de dinero.

Las transacciones financieras tradicionales, que antes dependían del dinero en efectivo o de instrumentos relacionados con el efectivo, ahora adoptan nuevas tecnologías como Internet, los pagos móviles y los sistemas de tarjetas, ganando rápidamente aceptación en todo el mundo. Estos avances no solo repercuten en las técnicas de investigación existentes y las estrategias de prevención de delitos financieros, sino que también ponen en tela de juicio la eficacia de las prácticas del pasado como el efectivo, los cheques y las cuentas bancarias, que dependían en gran medida de estrictos protocolos de conocimiento del cliente (KYC, por sus siglas en inglés).

La creciente evolución de las monedas digitales complica aún más el panorama, ofreciendo a los delincuentes vías para ocultar el origen de sus ganancias y transferir fondos a través de las fronteras de forma clandestina. Numerosas investigaciones recientes llevadas a cabo con éxito ponen de relieve la utilización de monedas digitales por parte de organizaciones delictivas para el blanqueo de capitales. Sin embargo, estos ejemplos también revelan que el rastreo de la propiedad de las monedas digitales, aunque complejo, no es imposible.

Las redes de moneda digital suelen mantener registros de transacciones en un libro mayor público distribuido, lo que permite a las herramientas de supervisión analítica detectar actividades sospechosas. Cada transacción digital deja un rastro y, con un escrutinio adecuado, se puede levantar el velo del secretismo, lo que permite a las autoridades identificar, localizar e incautar activos asociados a actividades ilícitas.

Sin embargo, esta cantidad de información no sirve de nada si no sabemos utilizarla adecuadamente; es crucial que las fuerzas del orden entiendan las criptomonedas para:

1. **Prevenir actividades ilícitas:** los delincuentes utilizan las criptomonedas cada vez con mayor frecuencia para diversas actividades ilícitas, como el blanqueo de capitales, el tráfico de drogas, la financiación del terrorismo y la ciberdelincuencia. Las fuerzas del orden deben comprender cómo funcionan estas monedas digitales para prevenir y combatir eficazmente dichas actividades delictivas.

2. **Investigación de delitos financieros:** A medida que los delincuentes recurren a las criptomonedas para ocultar sus ganancias ilícitas, las fuerzas del orden deben poseer los conocimientos y herramientas necesarios para investigar y rastrear estas transacciones. Comprender la tecnología subyacente y los métodos utilizados por los delincuentes ayuda a las autoridades a rastrear y perseguir a los implicados en delitos financieros.

Para prepararse para el futuro, las fuerzas del orden deben adquirir conocimientos sobre las criptomonedas, la red oscura («dark web») y las técnicas de cifrado; deben ser capaces de reconocer los indicadores de participación en criptomonedas, como la presencia de iconos de criptomonederos en dispositivos electrónicos, el uso de monederos, visitas a los cajeros automáticos y quioscos de criptomonedas y transacciones entre personas interesadas e intercambios de criptomonedas.

Este manual sirve como un recurso integral, que dota al personal de las fuerzas del orden con los conocimientos, las herramientas y las mejores prácticas necesarias para investigar y abordar eficazmente los delitos relacionados con las criptomonedas, salvaguardando en última instancia a las comunidades y defendiendo el estado de Derecho en la era digital.

2. Comprender las criptomonedas

Este capítulo proporciona una exploración en profundidad de los aspectos fundamentales y los atributos distintivos de las criptomonedas, ofreciendo a los lectores una comprensión completa de estos innovadores activos digitales. En el punto central de este debate residen los principios fundamentales que sustentan las criptomonedas y que constituyen los cimientos sobre los que descansan su funcionamiento y su importancia.

Uno de los conceptos clave en los que se hace hincapié es la naturaleza descentralizada de las criptomonedas, que las distingue de las formas tradicionales de moneda controladas por las autoridades centrales. Esta descentralización se ve facilitada por la tecnología de «blockchain», un sistema de tecnologías de registro distribuido (DTL) que registra y verifica las transacciones a través de una red de nodos, lo que garantiza la transparencia, la seguridad y la inmutabilidad.

Además de explorar los aspectos técnicos de las criptomonedas, el capítulo presenta a los lectores y lectoras el dinámico panorama legislativo internacional que rige estos activos digitales. Esto incluye una descripción general de los marcos reglamentarios, los requisitos de cumplimiento y las consideraciones jurisdiccionales que repercuten en el uso, el comercio y la fiscalidad de las criptomonedas en las distintas jurisdicciones.

2.1. Estructura y características básicas

Las criptomonedas representan activos digitales que facilitan las transacciones remotas y semiautónomas, eliminando la necesidad de un intermediario centralizado. A diferencia de las monedas tradicionales emitidas y reguladas por gobiernos o instituciones financieras, las criptomonedas operan en redes descentralizadas. Estas redes están formadas por participantes voluntarios, incluidos particulares y organizaciones, que ejecutan servidores informáticos que gestionan colectivamente las transacciones a través de un protocolo de gobernanza compartido, normalmente implementado como un algoritmo de *software*.

Esta estructura descentralizada garantiza que ninguna entidad o persona física pueda ejercer control sobre todo el sistema. En consecuencia, no existe una autoridad centralizada ni un intermediario con el que las fuerzas del orden puedan interactuar

en las transacciones de criptomonedas. En cambio, los usuarios y usuarias que desean realizar transacciones necesitan acceder a un *software* específico conocido como monedero, junto con un código alfanumérico único denominado clave privada. La clave privada sirve como mecanismo de autenticación similar a una contraseña, que permite a los usuarios acceder y gestionar de forma segura sus tenencias de criptomonedas. Para muchos usuarios, los monederos son accesibles a través de aplicaciones para teléfonos inteligentes, que no solo facilitan las transacciones sino que también administran claves privadas y direcciones de los monederos.

En cuanto a la naturaleza de las transacciones con criptomonedas, es esencial destacar los principios criptográficos subyacentes a su seguridad. Las transacciones se cifran y autentican a través de algoritmos matemáticos complejos, lo que garantiza la integridad y confidencialidad de cada transacción. Esta capa criptográfica proporciona un nivel sólido de seguridad, mitigando el riesgo de acceso no autorizado y actividad fraudulenta.

Además, la naturaleza descentralizada de las redes de criptomonedas fomenta la transparencia y la cooperación entre los participantes de la red. Cada transacción se registra en un libro de contabilidad público conocido como «blockchain», que se distribuye entre múltiples nodos dentro de la red. Esta tecnología de registro distribuido (DTL) garantiza la transparencia y la inmutabilidad, ya que las transacciones no se pueden alterar ni manipular una vez registradas.

En octubre de 2008, apareció en Internet un artículo innovador, atribuido a una entidad llamada “Satoshi Nakamoto”. Este artículo, titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (un sistema de dinero en efectivo electrónico *peer-to-peer)*[2], presentó un concepto innovador: el uso de una red de igual a igual para establecer un sistema descentralizado de transacciones electrónicas, eliminando la necesidad de intermediarios y fomentando las transacciones sin confianza. Esta idea revolucionaria presentó al mundo *bitcoin*, una moneda digital diseñada para operar independientemente de las instituciones financieras tradicionales y las autoridades centralizadas. La visión de Satoshi Nakamoto describió un marco en el que las personas físicas pudieran realizar transacciones entre sí de forma segura y directa, sin necesidad de supervisión de terceros.

El 3 de enero de 2009, la red Bitcoin inició oficialmente sus operaciones con el lanzamiento del *software* cliente Bitcoin de código abierto inaugural y la creación del primer *bitcoin*. Esto marcó el origen de una nueva era en las finanzas, donde las monedas digitales descentralizadas ganaron protagonismo y desafiaron las nociones convencionales de intercambio monetario y confianza. La aparición del *bitcoin* no solo introdujo un enfoque novedoso de las transacciones financieras, sino que también desencadenó un fenómeno global, inspirando la creación de numerosas criptomonedas alternativas y proyectos basados en «blockchain».

El *software* de la red funciona sobre una base de código abierto, lo que significa que su código es de libre acceso para el público, lo que invita a contribuciones y mejoras de desarrolladores de todo el mundo. A diferencia de los sistemas privados, este

2. Disponible en https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

software no es propiedad ni está gobernado por ninguna entidad única, sino por una comunidad colaborativa de personas físicas dedicadas a su mantenimiento y mejora.

En las criptomonedas basadas en pruebas de trabajo, la gestión y validación de las transacciones, así como la creación de nuevas monedas, se realizan de forma colectiva por los participantes en la red, quienes aportan voluntariamente la potencia computacional de sus máquinas. Este esfuerzo colectivo, conocido como *minería*, implica la verificación y el registro de transacciones en un libro de contabilidad público, denominado «blockchain». Este libro de contabilidad sirve como registro permanente e inmutable de cada transacción realizada en la red. A través del proceso de minería, se incentiva a los participantes de la red a validar las transacciones y mantener la integridad de la «blockchain». A cambio de sus contribuciones, los mineros son recompensados con *bitcoins* recién generados, así como con las comisiones asociadas a las transacciones procesadas. Este mecanismo de recompensa no solo incentiva la participación activa en la red sino que también garantiza la seguridad y estabilidad del sistema descentralizado.

Las transacciones criptográficas entre pares suelen implicar el uso de identificadores únicos conocidos como *direcciones*, cadenas de caracteres alfanuméricos como 12c6DSiU4Rq3P4ZxziKxzr- L5LmMBrzjrJX[3].

Cuando un usuario instala una aplicación criptográfica o inicializa un monedero, el *software* genera automáticamente una serie de direcciones junto con el correspondiente par de claves criptográficas . Los usuarios de criptomonedas tienen la flexibilidad de generar múltiples direcciones según sea necesario. Para mejorar la privacidad, los usuarios a menudo utilizan las direcciones solo una vez antes de deshacerse de ellas. Cada transacción registrada en el «blockchain» asocia un saldo a una dirección específica y a su correspondiente par de claves pública y privada.

La propiedad y el control de los criptoactivos están vinculados a la posesión de la clave privada asociada a una dirección concreta. De manera similar al uso de una contraseña para acceder a una cuenta bancaria, las personas físicas pueden gastar criptomonedas firmando transacciones con sus claves privadas. Las transacciones se pueden iniciar y completar mediante el *software* cliente instalado en varios dispositivos, como ordenadores, teléfonos inteligentes, tabletas y *hardware* dedicado.

Cuando un usuario inicia una transacción, la información se transmite a la red, donde se somete a validación. La red verifica la validez de la transacción confirmando que ha sido firmada correctamente con la clave privada correcta y que el valor transferido no se ha gastado previamente. Dado que el saldo asociado a una dirección es esencialmente un registro de transacciones pasadas almacenadas en el libro de contabilidad público («blockchain»), no hay “monedas” físicas implicadas y el *software* cliente utilizado para las transacciones no almacena ningún valor monetario.

---

3. Todas las direcciones y claves privadas mencionadas en este manual tienen únicamente fines de aprendizaje y nunca deben utilizarse en la práctica. El envío de criptomonedas a las direcciones mencionadas o el uso de las claves privadas mostradas puede provocar la pérdida permanente de las monedas enviadas.

Es importante señalar que las criptomonedas existen puramente como entradas en la «blockchain», y su propiedad depende de la posesión de la clave privada necesaria para autorizar las transacciones. Este concepto plantea importantes retos y preocupaciones en los casos en que es necesario incautar *bitcoins* asociados a actividades delictivas, ya que la naturaleza digital de las criptomonedas complica los procedimientos tradicionales de incautación de activos.

2.2. Existen diferentes criptomonedas

A raíz de la creación de *Bitcoin* hace más de una década, han surgido una gran cantidad de nuevas variantes de criptomonedas, lo que ha contribuido al panorama diverso de activos digitales disponibles en la actualidad. Establecer un recuento exacto resulta complicado, dada la naturaleza dinámica y en constante evolución del mercado de criptomonedas. Sin embargo, incluso las estimaciones más conservadoras parecen indicar que el número de criptomonedas distintas actualmente en circulación se cuenta por miles. Las criptomonedas operan en plataformas distintas, cada una con su propia infraestructura de «blockchain» y, por lo general, no pueden intercambiarse directamente sin mecanismos intermediarios como los puentes. Esta separación inherente implica que no se puede, por ejemplo, transferir Ethereum a una dirección *Bitcoin* o enviar *Bitcoin* a una dirección de Ethereum. Intentar hacerlo provocaría la pérdida de los activos involucrados. Para garantizar el éxito de una transferencia de fondos, es imprescindible utilizar la dirección de criptomoneda adecuada correspondiente al libro de contabilidad o red de «blockchain» específicos.

Para evitar errores, puede ser útil echar un vistazo a las criptomonedas más comunes y su formato de dirección.

Bitcoin

Tiene su origen en un libro blanco publicado en 2008 y se presenta como la primera criptomoneda reconocida a nivel mundial. Conserva su posición como la forma más destacada de moneda digital. Al operar en su «blockchain» específica, las transacciones de *bitcoin* se someten a la verificación de una red descentralizada de mineros que también generan nuevos *bitcoins*, respetando un límite predeterminado y fijo (se crearán 21 millones de *bitcoins* en total).

En la red Bitcoin, *prueba de trabajo* (PoW) es el mecanismo de consenso utilizado para validar transacciones y garantizar la «blockchain». En esencia, ciertos nodos de la red, llamados mineros, compiten para crear un nuevo bloque resolviendo un complejo rompecabezas matemático. Este rompecabezas, conocido como el "rompecabezas *hash*", consiste en procesar repetidamente los datos del bloque hasta encontrar un valor *hash*[4] que cumpla un determinado objetivo de dificultad establecido por la red. Una vez que un minero encuentra un valor *hash* que cumple el objetivo de

4. El *hashing* es el proceso de convertir datos (texto, números, archivos) en una cadena de letras y números de longitud fija. Los datos se convierten en estas cadenas de longitud fija, o valores *hash*, mediante un algoritmo especial llamado función *hash*.

dificultad, transmite el nuevo bloque a la red. Este bloque contiene las transacciones que el minero ha verificado y agrupado. El minero que haya extraído con éxito el bloque es recompensado con una cierta cantidad de *bitco*ins recién creados, así como con cualquier gasto de transacción incluido en el bloque. Esto sirve como incentivo para que los mineros gasten recursos computacionales y protejan la red.

> Las direcciones siempre empiezan por **1, 3 o bc1**. Su longitud varía entre 26 y 35 caracteres; ejemplo: **bc1q0v4qz095ftv72mcgql0yy39783keztj9fptupv.**

Ethereum

Ether es la criptomoneda que se ejecuta en la «blockchain» Ethereum. *Ether* opera en su propia «blockchain», pero a diferencia de *Bitcoin*, *Ether* no tiene límite, lo que significa que, en teoría, se puede crear una cantidad infinita de monedas. Ethereum también admite contratos inteligentes, que son programas que se ejecutan en la «blockchain» Ethereum y lo hacen automáticamente cuando se cumplen ciertas condiciones.

La «blockchain» Ethereum, a través de contratos inteligentes, permite la creación de otras criptomonedas (*tokens* fungibles), conocidas como t*okens* ERC-20. Los desarrolladores pueden crear *tokens* habilitados para contratos inteligentes que se pueden utilizar con otros productos y servicios.

Ethereum y los contratos inteligentes permiten la creación de otro tipo de *tokens*, conocidos como ERC-721 o *tokens* no fungibles (los **NFT**): estos *tokens* no son fungibles, lo que significa que no se pueden intercambiar de manera individualizada debido a sus propiedades únicas. Son similares a las unidades de moneda de «blockchain», excepto que están conectadas a archivos digitales únicos, de modo que se puede considerar que los *tokens* individuales tienen una distinción significativa de otros. Esta distinción proporciona a los NFT características y casos de uso únicos, como:

1. **Posesión:** ERC-721 permite a los usuarios poseer, transferir y supervisar de forma segura activos digitales únicos, garantizando registros de propiedad transparentes y verificables.
2. **Compatibilidad:** Esta norma garantiza una interacción fluida de los NFT con varios mercados de la red Ethereum, monederos y aplicaciones descentralizadas (dApps), enriqueciendo su funcionalidad y accesibilidad.
3. **Excepcionalidad y carácter distintivo:** A diferencia de los *tokens* fungibles, los NFT ERC-721 representan elementos singulares con atributos distintivos, lo que los hace muy apreciados tanto entre coleccionistas como creadores.
4. **Protección de la propiedad intelectual:** Los NFT ERC-721 sirven como salvaguarda de los derechos de propiedad intelectual al proporcionar a los artistas y creadores documentación inmutable de sus creaciones, junto con mecanismos para controlar su uso y posteriores ventas.

5. **Posesión fraccionada:** Los NFT construidos según el estándar ERC-721 se pueden fragmentar en porciones más pequeñas y negociables, lo que abre vías para que un público más amplio invierta en activos de alto valor.

6. **Compatibilidad entre plataformas:** El aprovechamiento de una norma compartida facilita la utilización fluida de los NFT en diversas plataformas y aplicaciones, ampliando el alcance de posibles aplicaciones y utilidades.

La «blockchain» Etherum (y otras compatibles) también permiten la creación de **criptomonedas estables**, criptomonedas cuyo valor está vinculado o ligado al de otra moneda, mercancía o instrumento financiero. Las criptomonedas estables tienen como objetivo proporcionar una alternativa a la alta volatilidad de las criptomonedas más populares. Algunos ejemplos son Tether (USDT), USD Coin (USDC), Dai (DAI) y Binance USD (BUSD).

Ethereum mantiene y amplía su «blockchain» de transacciones a través de un sistema completamente diferente al utilizado por Bitcoin. Prueba de participación (PoS, por sus siglas en inglés) es un mecanismo de consenso para lograr un acuerdo sobre el estado de la red y validar las transacciones. A diferencia de PoW, que se basa en la potencia computacional y actividades de minería que consumen mucha energía, PoS opera según el principio de apostar las tenencias de criptomonedas para proteger la red. En un sistema PoS, los expendedores son elegidos para crear nuevos bloques y validar transacciones en función de la cantidad de criptomonedas que poseen y están dispuestos a bloquear como garantía, lo que se conoce como su apuesta. Esencialmente, cuantas más criptomonedas apueste un expendedor, mayor probabilidad tendrá de ser elegido para crear un nuevo bloque y obtener recompensas.

> Las direcciones de Ethereum siempre empiezan por **0x** y constan de 40 caracteres. Las redes compatibles con Ethereum como Polygon, BNB Chain, Fantom y Avalanche también utilizan este formato. Ejemplo: **0x675bB023e268dCC43F543620577bCacB73047f08.**

Monero

Monero es una criptomoneda centrada en la privacidad que prioriza el anonimato, la seguridad y la descentralización. Se lanzó en abril de 2014 como una bifurcación de *Bitcoin*. El desarrollo de Monero se rige por principios destinados a garantizar la confidencialidad de las transacciones y la privacidad de sus usuarios. Mediante el uso de técnicas criptográficas avanzadas, como firmas en anillo, transacciones confidenciales en anillo (RingCT) y direcciones ocultas, Monero oculta información de las transacciones como el remitente, el destinatario y el importe. Esto garantiza que las transacciones en la «blockchain» de Monero sean privadas y no vinculables, y la convierte en una herramienta que cada vez más delincuentes utilizan para blanquear los productos del delito.

> Las direcciones de Monero siempre empiezan por **4 u 8**, y tienen 95 caracteres de longitud.

Ejemplo:
888tNkZrPN6JsEgekjMnABU4TBzc2Dt29EPAvkRxbANsAnjyPbb3iQ1Y-BRk1UXcdRsiKc9dhwMVgN5S9cQUiyoogDavup3H.

2.3. Monederos de criptomonedas y cómo gestionar transacciones de criptomonedas

Los monederos de criptomonedas, ya sea en forma de aplicaciones de *software* o de dispositivos físicos, sirven como repositorios seguros para las claves criptográficas necesarias para acceder y administrar los activos digitales dentro de una red de «blockchain» específica. A diferencia de los monederos tradicionales que contienen moneda física, los monederos de criptomonedas protegen las claves vitales necesarias para almacenar y transferir criptomonedas; en esencia, se encargan de almacenar de forma segura las **claves privadas**. Como activos digitales que residen únicamente en la tecnología de «blockchain», las criptomonedas se asocian a claves públicas y privadas en el momento del registro del monedero.

Estas claves sirven como credenciales criptográficas, validando la propiedad de las criptomonedas y facilitando el acceso a los activos asociados.

Garantizar la seguridad e integridad de estas claves es primordial, ya que son el eje de la propiedad de las criptomonedas y la autorización de transacciones. Los propietarios deben tener mucho cuidado para almacenar de forma segura sus claves y proteger sus monederos de criptomonedas mediante sólidas medidas de seguridad y prácticas de gestión diligentes. Proteger estas claves contra el acceso no autorizado, pérdida o robo es esencial para salvaguardar nuestros activos digitales. Por lo tanto, es fundamental emplear protocolos de seguridad estrictos y tener cuidado al administrar monederos de criptomonedas para mantener la integridad y la accesibilidad de las tenencias de criptomonedas.

Es fundamental que las fuerzas del orden comprendan qué son los monederos de criptomonedas debido a su papel central a la hora de facilitar y gestionar los activos digitales. Los monederos contienen información valiosa que puede ayudar a las fuerzas del orden en las investigaciones criminales. El historial de transacciones y las direcciones del monedero pueden proporcionar información importante sobre las transacciones financieras ilícitas, sistemas de blanqueo de capitales y otras actividades delictivas. El personal de las fuerzas del orden con conocimientos sobre carteras de criptomonedas puede aprovechar esta información para construir casos, identificar sospechosos y desmantelar redes delictivas. Además, comprender cómo funcionan los monederos de criptomonedas permite a las autoridades navegar de manera efectiva por el proceso de incautación y recuperación de fondos obtenidos ilícitamente.

En líneas generales, los monederos de criptomonedas se dividen en dos categorías: monederos calientes y monederos fríos (o de *hardware*). Los monederos calientes existen únicamente en formato digital y están constantemente conectados a Internet, lo que los hace más susceptibles a la piratería informática y a los ataques de

suplantación de identidad. Por otro lado, los monederos de *hardware*, un subconjunto de los monederos fríos, son dispositivos físicos que funcionan sin conexión a Internet, lo que proporciona una capa adicional de seguridad contra intrusiones maliciosas.

Los monederos calientes ofrecen la comodidad de la accesibilidad digital desde cualquier dispositivo conectado a Internet. La mayoría de ellos se pueden descargar de forma gratuita y están disponibles como aplicaciones móviles o extensiones de navegador. Exodus y Trust Wallet son dos ejemplos de este tipo de monederos de moneda virtual. Una de las principales ventajas de estos monederos es su interfaz fácil de usar. Por otro lado, un monedero de almacenamiento en frío es un tipo de monedero de criptomonedas diseñado para almacenar claves privadas fuera de línea, lo que proporciona una capa adicional de seguridad contra la piratería informática, los ataques de programas maliciosos («malware») y otras amenazas a la seguridad. Las claves privadas se utilizan para acceder y administrar los activos de criptomonedas. Al almacenarlas fuera de línea, los monederos fríos dificultan el acceso de agentes maliciosos a sus activos digitales.

La forma más simple de **almacenamiento en frío** se conoce como un **monedero de papel**, que es esencialmente un documento físico que contiene tanto la dirección como su clave privada. Cualquiera puede generar e imprimir el documento utilizando una de las herramientas de monedero de papel en línea existentes.[5], utilizando una impresora fuera de línea para mayor seguridad. Normalmente, el monedero de papel incluye un código QR, lo que permite escanearlo y firmarlo fácilmente para ejecutar transacciones.

Sin embargo, un inconveniente importante de este método es el riesgo de pérdida, daño o destrucción del papel. Si el monedero de papel se extravía, se vuelve ilegible o se daña, el usuario puede perder permanentemente el acceso a los fondos almacenados en la dirección asociada. Por lo tanto, es indispensable que las personas físicas que optan por este enfoque garanticen un almacenamiento seguro del monedero de papel, como el uso de una caja de seguridad u otro método de almacenamiento fiable.

Otro método de almacenamiento en frío implica el uso de **monederos de *hardware***, que utilizan un dispositivo fuera de línea o una tarjeta inteligente para generar claves privadas en un entorno fuera de línea. Un ejemplo de este enfoque es el Ledger USB Wallet, que utiliza una tarjeta inteligente para mejorar la seguridad de las claves privadas. Otros monederos de *hardware* destacables incluyen TREZOR y KeepKey. Estos monederos de *hardware*, que funcionan de manera similar a una unidad USB, requieren un ordenador y una aplicación para administrar y almacenar claves privadas sin conexión. Los dispositivos varían en complejidad, desde unidades de almacenamiento USB estándar hasta dispositivos sofisticados equipados con características como baterías, conectividad Bluetooth y *software* especializado.

Al igual que ocurre con los monederos de papel, es fundamental almacenar los monederos de *hardware* y las tarjetas inteligentes de forma segura para mitigar el riesgo de pérdida o daño, ya que cualquier suceso de este tipo podría provocar la

5. Por ejemplo, véase http://www.bitaddress.org/

pérdida permanente del acceso a los activos de criptomonedas almacenados. Por lo tanto, los usuarios deben actuar con diligencia para salvaguardar estos dispositivos e implementar medidas de seguridad adecuadas para proteger su riqueza digital.

La mayoría de los monederos, y todos los mencionados anteriormente excepto el monedero de papel, están protegidos por **frases de recuperación (semilla).**

Una frase **de recuperación (semilla**) sirve como medida de seguridad fundamental para recuperar monederos de criptomonedas perdidos o dañados y consta de una secuencia de 12 o 24 palabras generadas aleatoriamente. También conocida como frase mnemotécnica, actúa como salvaguarda de los activos digitales mantenidos bajo custodia personal. Tanto los monederos calientes como los fríos pueden emplear una frase semilla con fines de recuperación, lo que la convierte en una herramienta versátil en el ámbito de la seguridad de las criptomonedas. De manera similar a una contraseña maestra, la frase semilla de respaldo sirve como puerta de acceso a todas las criptomonedas asociadas con el monedero que la generó, incluso en casos en que el propio monedero se haya eliminado o perdido. Básicamente, funciona como un gestor de contraseñas para criptomonedas, proporcionando un medio seguro de recuperación en momentos de necesidad. Para mejorar la memorización, las frases semilla consisten en palabras simplificadas, generadas aleatoriamente y elegidas de una lista predeterminada de 2048 opciones. Esta elección de diseño garantiza que los usuarios puedan recordar fácilmente sus frases semilla sin necesidad de complejas secuencias numéricas o de caracteres especiales.

A continuación se muestra un ejemplo de una frase semilla de 12 palabras:

> *"arrepentirse, difícil, tímido, planeta, niño, ansiedad, típico, alternativo, humanidad, nunca, perder, llorar"*

2.4. Marco legislativo

En la última década, las criptomonedas, también conocidas como activos virtuales (los VA, por sus siglas en inglés) o criptoactivos (los CA), han trascendido sus orígenes de nicho para convertirse en un fenómeno generalizado con profundas implicaciones para el panorama financiero tradicional. Tanto particulares como empresas están adoptando cada vez más los VA para diversos fines, lo que refleja una creciente aceptación e integración de las monedas digitales en las finanzas convencionales. A nivel mundial, esta tendencia se ve subrayada por el creciente número de instituciones financieras que ofrecen servicios relacionados con los VA, lo que contribuye a la aparición de proveedores de servicios de activos virtuales (VASP, por sus siglas en inglés).

Sin embargo, junto con este aumento del uso legítimo, se ha producido un incremento correspondiente de las actividades ilícitas que explotan el anonimato y la naturaleza sin fronteras de las criptomonedas. Los elementos criminales han reconocido rápidamente el potencial de los VA como herramienta para llevar a cabo un amplio

espectro de actividades ilegales, que van desde el robo y el fraude básicos hasta sofisticados delitos transnacionales como el blanqueo de capitales y la financiación del terrorismo. Estas actividades nefastas presentan desafíos importantes para todos los actores involucrados en los esfuerzos de lucha contra el blanqueo de capitales (AML, por sus siglas en inglés), incluidas las autoridades reguladoras, las fuerzas del orden, las instituciones financieras y los proveedores de servicios de criptomonedas.

A medida que los VA continúan ganando terreno en la economía convencional, la necesidad de contar con medidas sólidas de lucha contra el blanqueo de capitales y una supervisión reguladora eficaz se hace cada vez más acuciante. Abordar el uso ilícito de criptomonedas exige esfuerzos de colaboración de todas las partes interesadas para desarrollar estrategias integrales, mejorar las capacidades de detección e implementar medidas de cumplimiento estrictas.

Uno de los principales organismos internacionales que ha intentado regular el mundo de los VA es el Grupo de Acción Financiera Internacional (GAFI). El GAFI, también conocido por su nombre en francés, Groupe d'Action Financière (GAFI), es una organización intergubernamental fundada en 1989 por iniciativa del G7 para desarrollar políticas de lucha contra el blanqueo de capitales y mantener ciertos intereses. En 2001, su mandato se amplió para incluir la financiación del terrorismo. Establece normas internacionales que tienen como objetivo prevenir estas actividades ilegales y el daño que causan a la sociedad. Las Recomendaciones del GAFI proporcionan un marco integral de medidas para ayudar a los países a hacer frente a los flujos financieros ilícitos. Incluyen un marco sólido de leyes, reglamentos y medidas operativas para garantizar que las autoridades nacionales puedan adoptar medidas eficaces para detectar e interrumpir los flujos financieros que alimentan la delincuencia y el terrorismo, y castigar a los responsables de actividades ilegales. Las Recomendaciones son la base sobre la cual todos los países deben alcanzar el objetivo compartido de luchar contra el blanqueo de capitales, la financiación del terrorismo y la financiación de la proliferación. El GAFI hace un llamamiento a todos los países para implementar eficazmente estas medidas en sus sistemas nacionales.

El GAFI también cuenta con organismos regionales, como el Grupo de Acción Financiera del Caribe (GAFIC), una organización de estados y territorios de la cuenca del Caribe que han acordado implementar contramedidas comunes contra el blanqueo de capitales y la financiación del terrorismo, o el Grupo de Acción Financiera de Latinoamérica (GAFILAT).

En octubre de 2018, el Grupo de Acción Financiera Internacional (GAFI) dio un paso importante al proporcionar sus definiciones inaugurales de los VA y los VASP, con el objetivo de delimitarlos del término "moneda virtual" empleado anteriormente. Estas nuevas definiciones se incorporaron a la Recomendación n.° 15 del GAFI, relativa a las "Nuevas tecnologías", con el objetivo principal de dilucidar las expectativas normativas impuestas a estas clases de activos emergentes y a sus proveedores de servicios:

> *Un activo virtual es una representación digital de valor que puede comercializarse o transferirse digitalmente y puede utilizarse con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiat, valores y otros activos financieros que ya están incluidos en otras partes de las Recomendaciones del GAFI*[6].

Al mismo tiempo, el GAFI dio una definición amplia de los VASP como se indica a continuación:

Por «proveedor de servicios de activos virtuales» se entiende toda persona física o jurídica que no esté contemplada en ninguna otra parte de las Recomendaciones y que, como empresa, realice 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 de activos virtuales; y*
> v. *participación y prestación de servicios financieros relacionados con la oferta y/o venta de un activo virtual por parte de un emisor.*

Las Recomendaciones del GAFI sirven como marco vital para la regulación y supervisión de las instituciones financieras, incluyendo los intercambios de criptomonedas entre otras entidades. Estas recomendaciones desempeñan un papel fundamental a la hora de establecer protocolos sólidos de lucha contra el blanqueo de capitales, salvaguardando así la integridad del sistema financiero y disuadiendo las actividades ilícitas. Además, crean el marco dentro del cual las fuerzas del orden pueden buscar y obtener información vital de los VASP.

Las bolsas de criptomonedas juegan un papel crucial a la hora de identificar y notificar actividades sospechosas a las autoridades competentes. Se les encomienda la aplicación de procedimientos para detectar y notificar transacciones que susciten preocupación sobre posibles actividades de blanqueo de capitales, financiación del terrorismo u otra conducta ilícita. Mediante la notificación oportuna de dichas actividades, las bolsas apoyan activamente iniciativas más amplias destinadas a combatir los delitos financieros.

2.5. Indicadores de alerta de activos virtuales

En los inicios de la industria de las criptomonedas, la transparencia no era una prioridad para las empresas de criptomonedas. Sin embargo, el panorama actual

6. GAFI, Recomendaciones del GAFI, febrero de 2023, pág. 135

experimenta un cambio significativo, y las empresas de criptomonedas ahora otorgan gran importancia a los procedimientos de conocimiento del cliente (KYC) y a las medidas de cumplimiento. El mayor escrutinio por parte de las autoridades nacionales e internacionales ha llevado a las empresas de criptomonedas a aplicar estrictos procesos de selección. Ahora se les exige que dispongan de sólidos sistemas de KYC para autenticar las identidades de los clientes, sus direcciones y las fuentes de sus fondos. Además, el seguimiento de las transacciones y la evaluación de los riesgos se han convertido en partes integrantes de sus requisitos operativos. La aplicación de estas medidas a menudo requiere la revisión de procesos existentes o el desarrollo de nuevos programas.

A pesar del desafiante camino para lograr el cumplimiento de la normativa, algunas bolsas optan por evitar las mejoras necesarias y continúan operando sin adherirse a las normas KYC. Este incumplimiento las hace vulnerables a actores delincuentes, tanto de las finanzas tradicionales como del espacio criptográfico, que buscan activamente plataformas que carecen de mecanismos de KYC adecuados para participar en actividades fraudulentas. Trabajar con bolsas de criptomonedas que no cumplen las normas plantea riesgos para los clientes, ya que sus fondos pueden estar en juego en el caso de un cierre obligatorio. Además, estas bolsas que no cumplen con las normas pueden carecer de medidas de seguridad adecuadas para salvaguardar los fondos y la información personal de los usuarios, lo que las hace susceptibles a diversos tipos de ataques.

Para las personas que trabajan en instituciones financieras convencionales, el concepto de activos virtuales y transacciones realizadas a través de VASP puede parecer desconcertante. Sin embargo, los signos de actividad ilícita se parecen mucho a los observados en las transacciones financieras tradicionales. Las señales de alerta en las transacciones de activos virtuales reflejan los indicadores reconocidos por los investigadores de lucha contra el blanqueo de capitales y los sistemas de supervisión de transacciones en las transacciones fiat. Detectar y abordar estas señales de alerta es crucial para mitigar el riesgo.

Hay seis señales de alerta principales identificadas por el GAFI[7]:

- **Indicadores de señales de alerta relacionados con las transacciones:** configurar transacciones de VA para pequeños importes o inferiores a los umbrales de mantenimiento de registros o notificaciones; realizar múltiples transacciones de alto valor; depositar los VA en una bolsa y luego retirarlos inmediatamente; aceptar fondos sospechosos de ser robados o fraudulentos;

- **Indicadores de señales de alerta relacionados con patrones de transacciones:** para iniciar una nueva relación con un VASP, efectuar un gran depósito inicial y financiar la totalidad de la apuesta el primer día de apertura; operaciones que impliquen el uso de más de un VA sin una explicación correcta y plausible; realizar transferencias frecuentes a la misma cuenta de VA por más de

7. FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, GAFI, París, Francia. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red- Flag-Indicators.pdf

una persona, por una o más personas desde la misma dirección IP, o por grandes cantidades de dinero en un período determinado;

- **Indicadores de señales de alerta relacionados con el anonimato:** actividad transaccional anómala de VA convertidos en efectivo en intercambios desde monederos asociados a la plataforma P2P sin ninguna explicación lógica; VA transferidos hacia o desde monederos que muestran patrones de actividad previos relacionados con el uso de mezcladores de los VASP o plataformas P2P; transacciones que utilizan servicios de mezcla que sugieren la intención de mover fondos ilegales entre direcciones de monederos conocidas y mercados de la red oscura («dark web»); usuarios que registran nombres de dominio de Internet en la plataforma de VASP a través de servidores proxy para ocultar o eliminar propietarios de nombres de dominio; recepción o envío de dinero a VASP cuyos procesos de CCD o KYC son débiles o inexistentes;

- **Indicadores de señales de alerta sobre remitentes o destinatarios:** crear cuentas separadas bajo diferentes nombres para eludir las restricciones sobre los límites de negociación o retirada de fondos impuestos por los VASP; transacciones iniciadas desde direcciones IP no fiables, direcciones IP de jurisdicciones sancionadas o direcciones IP previamente marcadas como sospechosas; intentos frecuentes de abrir una cuenta dentro del mismo VASP desde la misma dirección IP; ausencia o insuficiencia de información de KYC o un cliente que niega solicitudes de documentos de KYC o preguntas sobre el origen de los fondos;

- **Indicadores de señales de alerta relacionados con el origen de los fondos o del patrimonio:** transacciones derivadas de o para servicios de juegos de azar en línea; falta de transparencia o información insuficiente sobre el origen y los propietarios de los fondos, como fondos colocados en ofertas iniciales de monedas (ICO) o sistema de pago en línea con tarjetas de crédito/prepago seguido de retirada instantánea; uso de una o más tarjetas vinculadas a un monedero de VA para retirar grandes cantidades de moneda fiat;

- **Indicadores de señales de alerta relacionados con riesgos geográficos:** los fondos del cliente se originan o se envían a una bolsa que no está registrada en la jurisdicción del cliente; el cliente envía dinero a VASP que operan en jurisdicciones que carecen de regulaciones sobre VA o que implementan controles de AML / CFT; el cliente establece o traslada oficinas en jurisdicciones que carecen de regulaciones legales que rigen los VA.

2.6. Regla de viaje

De especial importancia para las criptomonedas es la aplicación de la Recomendación n.° 16, que hace extensiva la llamada regla de viaje a los VA. Obliga a los VASP a obtener y revelar información precisa sobre el remitente y el destinatario de una transferencia de activos virtuales a los VASP homólogos o a las instituciones financieras, ya sea durante la transacción o antes de ella. Mediante la recopilación de

estos datos, las autoridades pueden identificar comportamientos sospechosos, como transferencias de fondos en las que participen personas físicas o entidades vinculadas a actividades delictivas, y posteriormente adoptar las medidas necesarias para frustrar o procesar acciones ilegales.

Dado que la información personal de las partes implicadas en las transacciones acompaña a sus transferencias, esta normativa ha sido denominada la "Regla de Viaje". El GAFI propone[8] que los países apliquen un umbral de minimis de 1000 USD/EUR para las transferencias de VA, aunque reconoce que habría relativamente menos requisitos para las transferencias de VA por debajo de este umbral en comparación con las que lo superen.

En el caso de las transferencias de VA que se sitúen por debajo del umbral, los VASP deben recopilar:

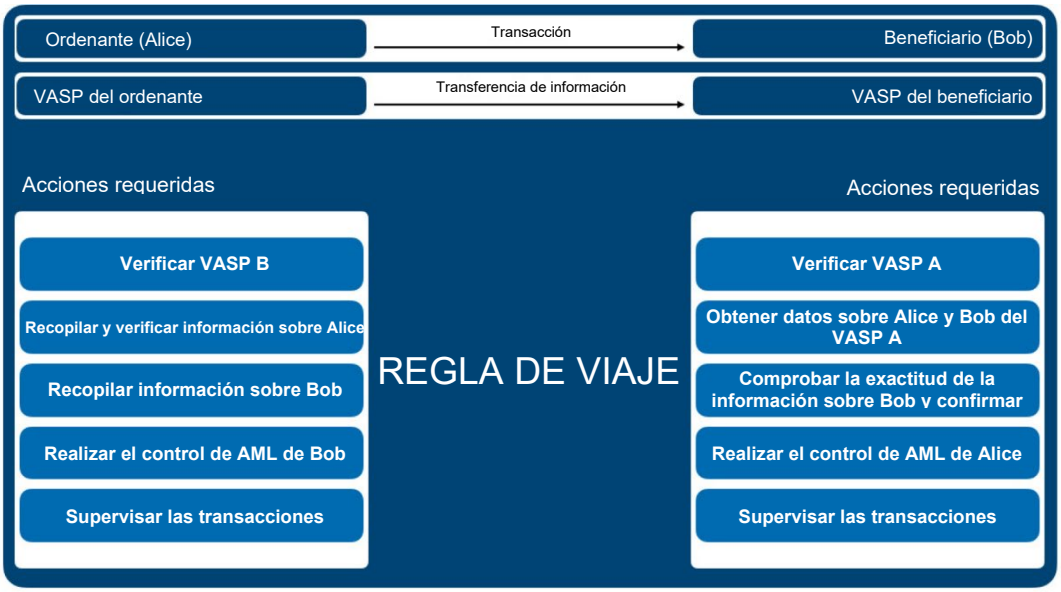
- Los nombres tanto del ordenante (remitente) como del beneficiario (destinatario)
- La dirección del monedero del activo virtual (VA) para cada transacción o un número de referencia de transacción único.

La verificación de dicha información no es obligatoria a menos que se observen circunstancias sospechosas relacionadas con el blanqueo de capitales/la financiación del terrorismo (MLCTF), en cuyo caso se deberá verificar la información sobre el cliente.

Para las transferencias que superen el umbral, los VASP están obligados a recopilar:

- Nombre del ordenante
- Número de cuenta del ordenante de la cuenta utilizada para procesar la transacción (p. ej., dirección del monedero)
- Dirección física (geográfica) del ordenante; número de identidad nacional; número de identificación del cliente (es decir, no un número de transacción) que identifica de manera exclusiva al ordenante ante la entidad ordenante; o fecha y lugar de nacimiento
- Nombre del beneficiario
- Número de cuenta del beneficiario de la cuenta utilizada para procesar la transacción (p. ej., dirección del monedero)

8. FATF *(2022) Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, GAFI, París, Francia, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf



La recomendación 16 se aplica a los VASP siempre que sus transacciones, tanto en moneda fiat como en activos virtuales, incluyan:

- Transferencias electrónicas tradicionales
- Transferencias de VA entre un VASP y otra entidad obligada (como entre dos VASP o entre un VASP y otra entidad obligada como un banco o una institución financiera)
- Transferencias de VA entre un VASP y una entidad no obligada (es decir, un monedero no alojado)[9].

Dado que el GAFI se abstiene de respaldar una tecnología concreta de intercambio de datos, no existe un protocolo o red singular designado para la transferencia de datos. En consecuencia, ya existen varias redes para transferencias de datos cifrados, como OpenVASP, Shyft y Trisa. Sin embargo, estas redes siguen planteando problemas, como la compatibilidad de protocolos.

Más adelante, profundizaremos en cómo este marco legal faculta a las fuerzas de seguridad para rastrear transacciones delictivas anónimas en la «blockchain» hasta que llegan a un punto en el que se pueden emitir citaciones, obtener información e incautar activos.

9. Este escenario es único, ya que el GAFI no prevé que los VASP, al iniciar una transferencia de VA, proporcionen la información requerida a personas físicas que no son entidades obligadas (por ejemplo, a un monedero no alojado). Solo contadas jurisdicciones han aplicado esta parte.

3. Uso delictivo de criptomonedas

Dentro del intrincado panorama de las criptomonedas, se cierne un tema polémico: su explotación por parte de delincuentes para actividades ilícitas. Este capítulo profundiza en la dinámica polifacética de cómo las criptomonedas sirven como conducto para iniciativas nefastas, arrojando luz sobre los innumerables retos a los que se enfrentan las fuerzas del orden. El ascenso de los criptoactivos ha coincidido con un aumento en su utilización para actividades de blanqueo de capitales, proporcionando a los delincuentes un manto para ocultar los orígenes y destinos de los fondos ilícitos. Además, este capítulo explora la intrincada red de técnicas de ofuscación empleadas por los delincuentes, lo que complica aún más la tarea de rastrear las fechorías financieras. A medida que las criptomonedas siguen impregnando los sistemas financieros mundiales, la necesidad de contar con estrategias eficaces para combatir su uso indebido se vuelve cada vez más urgente.

3.1. Tráfico de drogas y blanqueo de capitales

Los narcotraficantes explotan las monedas virtuales y los pagos móviles entre pares debido al relativo anonimato que ofrecen, lo que complica los esfuerzos de detección. Estas transacciones, protegidas por un velo de anonimato (o, como veremos, seudonimato), presentan importantes retos a las fuerzas del orden que se esfuerzan por descubrir actividades ilícitas. Los activos virtuales se utilizan cada vez más en plataformas que facilitan el tráfico de drogas, lo que aumenta la complejidad de la lucha contra este atroz delito.

En 2023, el Departamento de Justicia de los Estados Unidos saltó a los titulares con la acusación contra cuatro hijos del narcotraficante mexicano encarcelado Joaquín “El Chapo” Guzmán. La acusación alegaba su implicación en el blanqueo de los beneficios de una operación de contrabando de fentanilo en los Estados Unidos mediante el uso de “criptomonedas imposibles de rastrear”. Simultáneamente, las autoridades estadounidenses anunciaron el mismo día la detención de un blanqueador de capitales en busca y captura en Guatemala. Según las autoridades, el individuo tenía vínculos con el cártel y fue acusado de recaudar 869 000 dólares en ganancias del tráfico de drogas, depositando posteriormente los fondos en monederos de criptomonedas. Estos casos de gran repercusión ponen de manifiesto la creciente tendencia de los cárteles de la droga y la delincuencia organizada en

Latinoamérica de adoptar monedas virtuales como medio para blanquear dinero, facilitar pagos y traficar con estupefacientes en la red oscura («dark web»).

Paralelamente a la proliferación de las monedas virtuales, han surgido mercados en línea como centros de tráfico sexual y mercancías ilegales. Estos mercados, a menudo ubicados en los recovecos de la "red oscura" («dark web»), representan un rincón clandestino de Internet accesible a través de *software* especializado como Tor, lo que fomenta un entorno de mayor anonimato para los usuarios que participan en transacciones ilícitas. El manto de secretismo de la red oscura («dark web») protege a los participantes del escrutinio, minimizando el riesgo de ser detectados por las fuerzas del orden.

Los mercados de la red oscura («dark web») son plataformas en línea dentro de la red oscura («dark web») que facilitan la compra y venta de diversos bienes y servicios. Estos mercados operan en redes anónimas y son conocidos por proporcionar cierto grado de anonimato tanto a compradores como a vendedores a través de tecnologías de cifrado y centradas en la privacidad. Aunque algunos artículos de estos mercados pueden ser legales, muchos están asociados con actividades ilegales, especialmente las drogas, lo que genera preocupación sobre la facilitación de empresas delictivas.

¿Cuáles son las características que hacen que los mercados de la red oscura («dark web») sean útiles frente a la actividad delictiva?

- **Anonimato:** Los mercados de la red oscura («dark web») operan en la red Tor, que permite a los usuarios acceder a sitios web con un mayor anonimato;
- **Transacciones en criptomonedas:** las transacciones en los mercados de la red oscura «dark web») suelen realizarse con criptomonedas como *Bitcoin*, Monero u otras monedas centradas en la privacidad. Esto añade una capa adicional de anonimato a las transacciones financieras;
- **Variedad de productos:** Los mercados de la red oscura («dark web») ofrecen una amplia gama de productos y servicios, tanto legales como ilegales. Los elementos legales pueden incluir herramientas centradas en la privacidad, bienes digitales o productos de nicho. Sin embargo, muchos mercados de la red oscura («dark web»)son conocidos por facilitar el comercio de artículos ilegales como drogas, armas de fuego, herramientas de piratería informática, datos robados y documentos falsificados;
- **Servicios de fondos en custodia:** Muchos mercados de la red oscura («dark web») utilizan servicios de fondos en custodia para facilitar las transacciones. En este proceso, los fondos son retenidos por un tercero (fondos en custodia) hasta que el comprador recibe el producto o servicio y queda satisfecho, tras lo cual los fondos se liberan al vendedor;

Los mercados de la red oscura («dark web»)plantean desafíos difíciles a las fuerzas del orden debido al anonimato de los usuarios y al uso de criptomonedas. Sin embargo, las fuerzas del orden en todo el mundo están trabajando activamente para

rastrear y detener a los individuos involucrados en actividades ilegales en estas plataformas y tenemos muchas investigaciones satisfactorias que acabaron con mercados de la red oscura («dark web») como SilkRoad, Hydra, Monopoly, Wall Street Market y muchos más.

En el lado positivo, con estas nuevas tecnologías y el crecimiento de la información digital disponible, los investigadores ahora tienen acceso a ingentes cantidades de datos, incluida la actividad digital, el tráfico de Internet, datos de navegación, registros telefónicos, actividades en redes sociales, correos electrónicos y, finalmente, la actividad de «blockchain». Aunque esta abundancia de información puede ser valiosa, también plantea desafíos importantes. La sobrecarga de información en las investigaciones criminales se refiere a la abrumadora cantidad de datos e información que los investigadores tienen que analizar mientras intentan resolver un delito.

La sobrecarga genera varias preocupaciones:

- **Volumen de datos:** El gran volumen de datos generados en la sociedad moderna puede ser inmenso. Recopilar, organizar y analizar estos datos es un proceso que lleva mucho tiempo y los investigadores pueden tener dificultades para mantenerse al día con la cantidad cada vez mayor de información disponible;
- **Retos tecnológicos:** Las fuerzas del orden pueden enfrentarse a desafíos en términos de infraestructura tecnológica, herramientas y experiencia. La rápida evolución de la tecnología hace necesario que los investigadores se mantengan actualizados sobre las últimas herramientas y técnicas para la gestión de pruebas digitales;
- **Limitaciones temporales:** Las investigaciones criminales suelen tener limitaciones temporales y los investigadores pueden no tener tiempo suficiente para examinar exhaustivamente todos los datos disponibles. Esto puede dar lugar a la posibilidad de pasar por alto información crucial.

Para contrarrestar esos problemas, los analistas e investigadores prestarán atención al seguimiento del ciclo de información, que es el proceso continuo y dinámico de recopilación, análisis y difusión de información a lo largo de las distintas etapas de una investigación. Implica el flujo sistemático de información procedente de diferentes fuentes, tanto internas como externas, y juega un papel crucial en la resolución de delitos.

El ciclo de información normalmente incluye las siguientes etapas:

- **Planificación:** identificar tareas, fuentes de información y planificar las diferentes fases de la investigación;
- **Recopilación:** los analistas e investigadores recopilan una amplia gama de datos y pruebas relacionadas con el delito. Esto puede incluir declaraciones de testigos, pruebas físicas, imágenes de vigilancia, análisis forenses e información obtenida de varias bases de datos y otras fuentes;

- **Evaluación:** no todas las pruebas recopiladas son útiles o relevantes; las fuerzas del orden deben centrarse en lo que puede aportar la solución al caso

- **Análisis:** a continuación se analizan los datos recopilados para identificar patrones, conexiones y posibles pistas. Esta etapa también implica la identificación de posibles lagunas o incoherencias.

- **Integración:** este paso implica la organización y el análisis de diversos datos y pruebas procedentes de múltiples fuentes para crear una comprensión integral y coherente de una investigación criminal. La integración es un aspecto fundamental de la aplicación de la ley moderna, especialmente dada la naturaleza diversa y a menudo compleja de la información disponible en los casos penales;

- **Difusión:** las fuerzas del orden suelen colaborar y compartir información entre sí para beneficiarse de la experiencia y los recursos colectivos. Esta colaboración puede implicar a agencias locales, estatales o federales, así como a otras entidades pertinentes.

ESTUDIO DE CASO: EJERCICIO DE ANÁLISIS EN LA INVESTIGACIÓN INTERNACIONAL SOBRE DROGAS	
Evaluar las fortalezas	Una organización delictiva vende drogas en la red oscura («dark web»), utilizando a sus miembros como vendedores
Evaluar las debilidades	Al configurar una cuenta de comprador falsa, los investigadores pueden recabar información sobre los vendedores e identificar las direcciones de criptomonedas utilizadas por la organización criminal. Se pueden seguir las transacciones en la «blockchain» para comprender qué intercambio está utilizando la banda
Oportunidad	En lugar de limitarse a detener a los vendedores de drogas, podemos desmantelar una organización criminal
Amenaza	La banda criminal está muy organizada y estructurada
Opción sostenible	Crear diferentes equipos, cada uno con una tarea específica (equipo técnico, equipo de análisis financiero, etc.)
Posibilidad deseable	La investigación proporcionará pistas sobre un grupo criminal organizado mayor
Teoría catastrófica	Una filtración alerta a los delincuentes que logran huir

	antes de ser detenidos
Proyecto de investigación	El inicio de la investigación
Organización operativa	Los equipos abrirán cuentas en el mercado de la red oscura («dark web»)
Objetivos operativos	Detener a todos los miembros del grupo criminal acusándolos tanto de tráfico de drogas como de blanqueo de capitales, identificando e incautando todos sus activos
Consideraciones y propuestas	Considerar el uso de los activos incautados para fines sociales
Resultados	Finalización de todas las tareas planificadas

3.2. Técnicas de ofuscación

Como se ha explicado anteriormente, la tecnología de «blockchain» actúa como un cambio de paradigma en el mantenimiento de registros, ofreciendo transparencia, inmutabilidad y accesibilidad sin precedentes. Este sistema de libro mayor descentralizado documenta meticulosamente cada transacción y la pone a disposición del público para su escrutinio. Cada transferencia está acompañada de metadatos exhaustivos, como marcas de tiempo, importes de las transacciones y los criptoactivos específicos utilizados. Aunque las identidades asociadas con las direcciones de «blockchain» permanecen ocultas detrás de seudónimos criptográficos, es fundamental reconocer la existencia de metodologías capaces de desentrañar estos seudónimos, un tema que exploraremos con mayor detalle más adelante.

A la luz de la transparencia inherente de las transacciones de «blockchain», particularmente en lo que respecta al movimiento de fondos ilícitos, los actores criminales han innovado sofisticadas estrategias y técnicas de ofuscación. Estas maniobras están meticulosamente diseñadas para frustrar los esfuerzos de investigación destinados a rastrear actividades nefastas dentro del ecosistema público de «blockchain». Estas estrategias, que van desde servicios de mezcla complejos hasta intrincadas técnicas de estratificación, introducen obstáculos formidables para las fuerzas del orden y los organismos reguladores encargados de luchar contra los delitos habilitados por «blockchain».

Dada la naturaleza polifacética de estas tácticas de evasión, los enfoques de investigación tradicionales pueden encontrarse mal equipados para navegar eficazmente por las complejidades de las actividades delictivas basadas en «blockchain». Como tal, existe una necesidad urgente de una evolución y adaptación continuas de las metodologías de investigación para abordar de manera eficaz los retos que plantea el panorama en rápida evolución de los delitos relacionados con «blockchain».

Antes de profundizar en técnicas de ofuscación más complejas, es importante destacar que, más allá de su utilización por parte de delincuentes y organizaciones criminales, existen numerosos casos de uso legítimo de estos métodos. Estas aplicaciones legítimas subrayan la versatilidad y el valor de las técnicas de ofuscación en diversos contextos, mostrando su adaptabilidad e importancia a la hora de abordar una amplia gama de retos y requisitos. Estas incluyen:

1. **Protección contra la vigilancia:** En una era en la que la privacidad digital está cada vez más amenazada, la capacidad de realizar transacciones privadas proporciona a las personas un escudo contra la vigilancia generalizada. Sin protección de la privacidad, toda transacción financiera se convierte en objeto de vigilancia, lo que potencialmente compromete la autonomía personal y financiera.

2. **Preservación de la confidencialidad financiera:** Al igual que las personas físicas esperan privacidad en sus transacciones financieras tradicionales, la misma expectativa se aplica a las transacciones de criptomonedas. Preservar la confidencialidad financiera es crucial para mantener la confianza y salvaguardar la información sensible del acceso no autorizado o la explotación.

3. **Prevención de la discriminación y elaboración de perfiles:** Sin garantías de privacidad, las personas corren el riesgo de ser objeto de prácticas discriminatorias o de elaboración de perfiles basados en su historial de transacciones. La capacidad de realizar transacciones privadas ayuda a mitigar el riesgo de dicha discriminación y garantiza un trato equitativo para todos los participantes en el ecosistema de criptomonedas.

4. **Mayor seguridad:** Las características de privacidad en las transacciones de criptomonedas no solo protegen contra la vigilancia externa, sino que también mejoran la seguridad al reducir el riesgo de robo de identidad, fraude y ataques dirigidos. Al ocultar la información de las transacciones, las medidas de privacidad ayudan a mitigar la posibilidad de que actores maliciosos exploten vulnerabilidades y comprometan información sensible.

Mezcladores y tambores

Los mezcladores de criptomonedas («Crypto tumblers» o «Crypto blenders», en inglés) , son servicios que operan dentro del ámbito criptográfico. Su función es ocultar los orígenes y destinos de las transacciones de criptomonedas mezclándolas aleatoriamente con otras transacciones legítimas. Este proceso garantiza el anonimato de las transacciones, lo que dificulta que terceros, incluidas las fuerzas del orden, las rastreen fácilmente.

Los mezcladores aceptan criptoactivos de múltiples orígenes; estas monedas posteriormente se distribuyen a diferentes direcciones antes de llegar al destino final, cortando efectivamente la conexión entre la fuente y el destino de los fondos. Al utilizar algoritmos, los mezcladores crean grupos distintos y facilitan el intercambio de varias criptomonedas. Al ocultar la información del remitente y del receptor, los mezcladores dificultan a los investigadores la identificación de las direcciones de origen y destino.

Existen diferentes tipos de mezcladores: los mezcladores centralizados son operados por servicios privados de terceros en los que los usuarios confían para mezclar sus criptoactivos, mientras que los mezcladores descentralizados funcionan como protocolos entre pares con un proceso de mezcla automatizado.

Cuando se utilizan mezcladores centralizados, los usuarios transfieren sus fondos a direcciones de monedero controladas por estos mezcladores, pagan una cuota por servicio y especifican el destino. Una vez recibidos estos fondos, el mezclador los combina con los de otros usuarios en un fondo común y los redistribuye. Sin embargo, los mezcladores centralizados plantean el riesgo adicional de depositar la confianza en un tercero. Existe un riesgo potencial de perder los fondos si la red o la compañía dejan de funcionar. Además, debido al importante volumen de fondos que manejan, los mezcladores centralizados se convierten en objetivos principales para los piratas informáticos y también pueden presentar riesgos de comportamiento malicioso por parte de la propia empresa. Algunos mezcladores centralizados pueden incluso almacenar información de los usuarios de forma privada, comprometiendo el anonimato que pretenden proporcionar. La eficiencia de los mezcladores centralizados aumenta con el número de usuarios, ya que una mayor base de usuarios reduce la probabilidad de detección.

Los mezcladores descentralizados utilizan protocolos de código abierto como CoinJoin para facilitar un proceso de mezcla automatizado y sin permisos. Se basan en la participación de múltiples usuarios en el protocolo, consolidando sus fondos en una única gran transacción y dirigiendo diferentes *Bitcoins* a varias direcciones de destino.

En los mezcladores sin custodia, una característica común conlleva la utilización de contratos inteligentes públicamente verificables y transparentes o computación multipartita segura para sustituir la necesidad de una entidad mezcladora de confianza. El proceso de mezcla sin custodia suele implicar dos pasos. Inicialmente, los usuarios depositan una cantidad idéntica de Ether (ETH) u otros *tokens* en un contrato de mezclador desde una dirección. Posteriormente, tras un intervalo de tiempo definido por el usuario, pueden retirar sus monedas depositadas a través de una transacción de retirada a una nueva dirección; mientras tanto, las criptomonedas se mezclan de diferentes maneras.

Para hacer frente a estos retos, las naciones de todo el mundo han aplicado medidas normativas dirigidas a los mezcladores de criptomonedas debido a su participación en transacciones financieras. En los Estados Unidos, por ejemplo, la Financial Crimes Enforcement Network (FinCEN) obliga a todos los mezcladores a cumplir los requisitos de registro establecidos en la Ley de secreto bancario (Bank Secrecty Act).

Además, en el año 2022, la Oficina de Control de Activos Extranjeros de los Estados Unidos ("OFAC", por sus siglas en inglés) tomó medidas decisivas al imponer sanciones a destacados mezcladores de criptomonedas como Tornado Cash y Blender.io. La OFAC administra y aplica sanciones económicas y comerciales basadas en la política exterior y los objetivos de seguridad nacional de los Estados Unidos contra países y regímenes extranjeros específicos, terroristas, narcotraficantes internacionales, aquellos que participan en actividades relacionadas

con la proliferación de armas de destrucción masiva y otras amenazas a la seguridad nacional, la política exterior o la economía de los Estados Unidos.

Según declaraciones del Departamento del Tesoro de los Estados Unidos, Tornado Cash se habría utilizado presuntamente en el blanqueo de más de 7000 millones de dólares desde su creación, mientras que Blender.io supuestamente estuvo implicado en la facilitación de actividades de blanqueo de capitales vinculadas a un grupo de piratas informáticos norcoreanos.

Estas sanciones van más allá de la mera prohibición a los individuos en los Estados Unidos de realizar negocios con los servicios antes mencionados; también implican el bloqueo de cualquier activo en poder de dichas entidades dentro de los Estados Unidos. Esta postura agresiva subraya el compromiso global de combatir las actividades financieras ilícitas facilitadas por los mezcladores de criptomonedas y sirve como elemento disuasorio contra su uso indebido en el futuro.

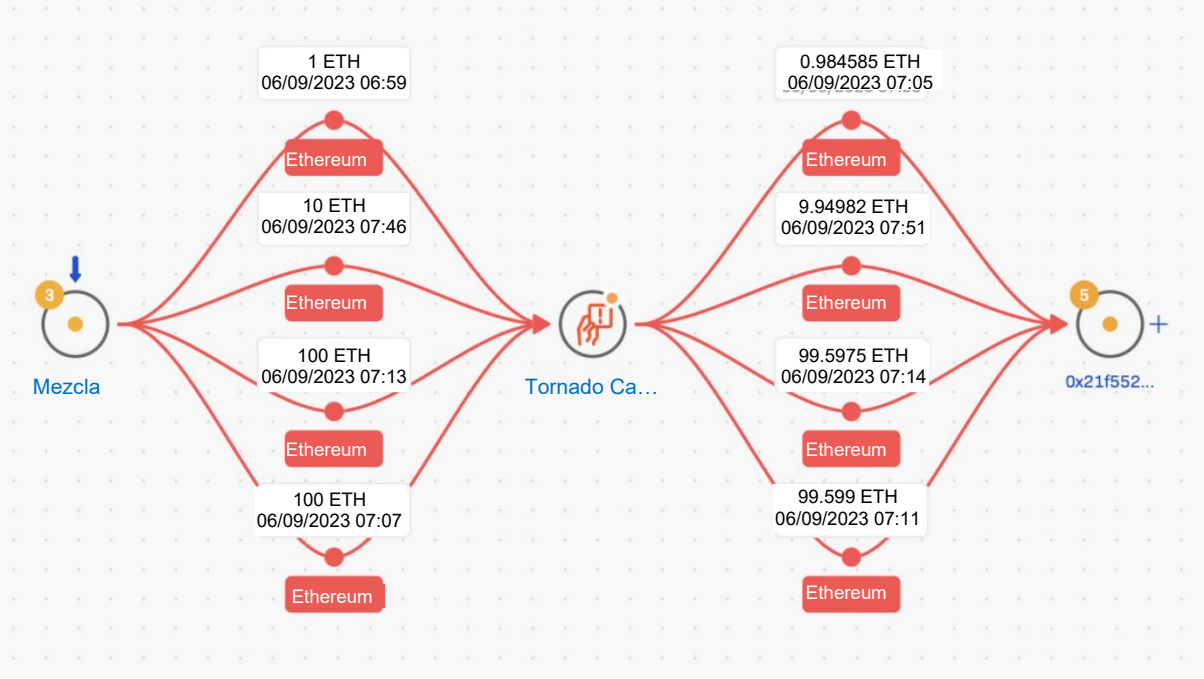


Figura 1: Ejemplo de fondos que pasan por un mezclador descentralizado (Tornado Cash) y se desanonimizan utilizando Crystal Expert, una herramienta de análisis de «blockchain» de Crystal Intelligence

Monedas de privacidad y salto de cadena

Las monedas de privacidad como Monero, Dash y Zcash han acaparado una atención significativa en recientes investigaciones criminales de alto perfil. La gran mayoría de los mercados de la red oscura («dark web»), incluido el ya desaparecido AlphaBay, aceptan de buen grado monero como pago por bienes y servicios. Además, las recientes medidas adoptadas por la OFAC ponen de relieve el uso creciente de monedas de privacidad por parte de los ciberdelincuentes en sus operaciones ilícitas.

Sin embargo, es importante tener en cuenta que no todas las monedas de privacidad conllevan el mismo nivel de riesgo en lo que respecta a facilitar el blanqueo de capitales y la financiación del terrorismo (ML/TF). Mientras que Monero cuenta con sólidas características de privacidad que la hacen resistente al análisis de «blockchain», otras monedas de privacidad como Zcash carecen de tales medidas de privacidad integradas. En consecuencia, las transacciones en las que intervienen estas monedas pueden ser examinadas por expertos en análisis de «blockchain», lo que permite la detección de posibles actividades ilícitas, de un modo similar a las transacciones en las que intervienen monedas que no son de privacidad.

Una estrategia común empleada por los actores criminales, a menudo junto con las monedas de privacidad, es la práctica de saltos de cadena. Esta táctica consiste en mover fondos entre diferentes criptomonedas y cadenas de bloques para ocultar el rastro de las transacciones. El GAFI destacó este riesgo emergente en 2022, subrayando su impacto potencial en los esfuerzos de lucha contra el blanqueo de capitales y la necesidad de una mayor supervisión normativa.

La prevalencia de los saltos de cadena ha aumentado en los últimos años, impulsada en gran medida por la proliferación de bolsas descentralizadas y servicios de "intercambio de monedas". Estas plataformas facilitan las transacciones entre pares y los intercambios de criptomonedas con controles mínimos o nulos de conocimiento del cliente, lo que permite a los participantes mantener un mayor nivel de anonimato. Esta tendencia plantea retos importantes a las autoridades policiales y reguladoras en sus esfuerzos por combatir la delincuencia financiera facilitada por las monedas de privacidad y los servicios financieros descentralizados[10].

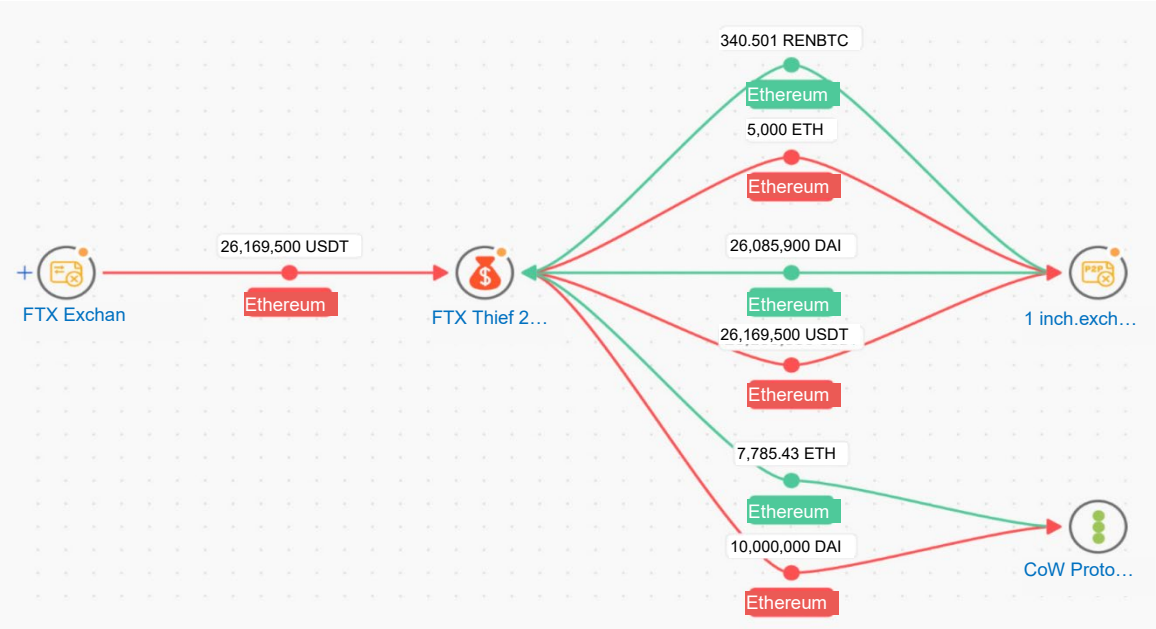


Figura 2 - Fondos robados de una importante casa de cambio e intercambiados por diferentes criptomonedas. Visualización mediante la herramienta Expert de Crystal Intelligence

10. https://crystalintelligence.com/thought-leadership/how-to-investigate-emerging-risks-related-to-cross-chain-crime/

Las herramientas de análisis de cadena de bloques desempeñan un papel crucial en la investigación de los saltos de cadena al proporcionar información sobre el movimiento de fondos entre diferentes criptomonedas y cadenas de bloques. Así es como estas herramientas pueden ayudar en la investigación:

1. **Seguimiento de transacciones:** Las herramientas de análisis de cadena de bloques pueden rastrear transacciones en múltiples cadenas de bloques, lo que permite a los investigadores seguir el flujo de fondos a medida que se mueven de una criptomoneda a otra. Al analizar el historial de transacciones y las direcciones asociadas, los investigadores pueden descubrir patrones y conexiones entre diferentes criptoactivos implicados en saltos de cadena.

2. **Agrupación de direcciones:** Estas herramientas emplean algoritmos sofisticados para agrupar direcciones que pertenecen a la misma entidad o monedero. Mediante la identificación de grupos de direcciones implicadas en actividades de salto de cadena, los investigadores pueden obtener una visión integral de las entidades implicadas y sus patrones de transacciones en varias criptomonedas.

3. **Reconocimiento de patrones:** Las herramientas de análisis de cadena de bloques pueden detectar patrones indicativos de saltos de cadena, como intercambios rápidos y frecuentes entre diferentes criptomonedas o el uso de plataformas de bolsas descentralizadas específicas conocidas por facilitar tales actividades. Al reconocer estos patrones, los investigadores pueden marcar transacciones sospechosas para un análisis más detallado.

4. **Puntuación de riesgo:** Algunas herramientas de análisis de «blockchain» ofrecen funciones de puntuación de riesgo que evalúan la probabilidad de que las transacciones estén asociadas con actividades ilícitas. Al asignar puntuaciones de riesgo a las transacciones implicadas en saltos de cadena, los investigadores pueden priorizar sus esfuerzos y centrarse en las transacciones de alto riesgo que justifican un escrutinio más minucioso.

5. **Visualización:** Las funciones de visualización en las herramientas de análisis de «blockchain» permiten a los investigadores e investigadoras visualizar el flujo de fondos en diferentes criptomonedas y cadenas de bloques. Al crear representaciones visuales de redes y relaciones de transacciones, los investigadores e investigadoras pueden obtener información sobre la complejidad de las actividades de salto de cadena e identificar los nodos o entidades clave implicados.

Es crucial elegir la herramienta adecuada para la investigación, dependiendo de las circunstancias y teniendo en cuenta las cadenas de bloques implicadas.

- La herramienta debe ser compatible con una amplia gama de criptomonedas y cadenas de bloques, desde las más populares como Bitcoin y Ethereum hasta las más utilizadas por los delincuentes como Tron;
- Debe poder proporcionar análisis sólidos, incluido el seguimiento de

transacciones, la agrupación de direcciones y la identificación de monederos. Las características como las visualizaciones gráficas son esenciales y pueden ayudar a ilustrar relaciones complejas,
- una interfaz fácil de usar es crucial, especialmente para los investigadores que pueden no ser expertos en «blockchain». La herramienta debe ofrecer una navegación intuitiva y visualizaciones claras;
- La supervisión en tiempo real y las alertas sobre actividades sospechosas pueden ser vitales para realizar investigaciones oportunas;
- Evaluar el modelo de precios para garantizar que se ajuste a las limitaciones presupuestarias y que al mismo tiempo ofrezca las funciones necesarias;
- Investigar la reputación de la herramienta dentro de la industria, incluidas las reseñas de los usuarios y los estudios de casos, para evaluar su fiabilidad y eficacia.

Soluciones de Capa 2

Las denominadas “soluciones de capa 2” en el contexto de «blockchain» se refieren a tecnologías o protocolos que se construyen sobre una red de «blockchain» existente (que constituyen la capa 1, como Bitcoin o Ethereum). El objetivo principal de las soluciones de Capa 2 es mejorar la escalabilidad, la eficiencia y la velocidad de la «blockchain» sin comprometer su seguridad o descentralización.

Estas soluciones gestionan transacciones fuera de la «blockchain» principal, lo que reduce la carga y la congestión en la Capa 1 y al mismo tiempo se benefician de sus características de seguridad. Esto también significa que a menudo las transacciones realizadas en la Capa 2 no son visibles, o no son completamente visibles, en la Capa 1.

Características clave de las soluciones de Capa 2

- **Procesamiento fuera de la cadena:** Las transacciones o los cálculos se trasladan de la cadena principal (Capa 1) a una capa secundaria. Este procesamiento fuera de la cadena reduce la carga de datos en la «blockchain» principal, aumentando su velocidad y eficiencia generales.

- **Escalabilidad mejorada:** Al procesar muchas transacciones fuera de la cadena principal, las soluciones de Capa 2 pueden aumentar significativamente la cantidad de transacciones por segundo que una red de «blockchain» puede manejar.

- **Reducción de las comisiones por transacción:** Dado que se procesan menos transacciones directamente en la «blockchain» principal, las comisiones por cada transacción suelen ser más bajas en las soluciones de C2.

- **Ventajas de seguridad:** Aunque las transacciones se procesan fuera de la cadena, la seguridad de estas soluciones aún depende de la «blockchain» de Capa 1 subyacente. En caso de disputa o necesidad de validación, la información de la transacción puede remitirse a la cadena principal.

Existen diferentes tipos de soluciones de Capa 2, con diferentes características. Las soluciones más comunes incluyen:

Canales de estado (red Lightning de Bitcoin, red Raiden de Ethereum): Los canales de estado permiten a dos partes crear un monedero multifirma y realizar muchas transacciones fuera de la cadena. Estas transacciones solo se registran en la «blockchain» cuando el canal está cerrado, lo que reduce la carga en la cadena principal.

Paquetes acumulativos (rollups): proceso que agrupa múltiples transacciones en un solo lote que se procesa fuera de la cadena. Los datos o pruebas de estas transacciones se envían después a la cadena principal en forma comprimida.

Cadenas laterales o sidechains (polígono): cadenas de bloques independientes que se ejecutan en paralelo a la «blockchain» principal (Capa 1). Tienen sus propios mecanismos de consenso y pueden operar de forma autónoma. Las transacciones en cadenas laterales se pueden liquidar periódicamente en la «blockchain» principal para mayor seguridad.

Las soluciones de Capa 2 abordan el *trilema* de escalabilidad en la tecnología de «blockchain», lo que sugiere que es un reto lograr escalabilidad, seguridad y descentralización al mismo tiempo. Al centrarse en la escalabilidad y aprovechar al mismo tiempo la seguridad y la descentralización de la cadena de Capa 1 subyacente, las soluciones de Capa 2 hacen que las cadenas de bloques sean más prácticas para su adopción masiva, especialmente para casos de uso como pagos, finanzas descentralizadas (DeFi) y NFT.

Aunque mejoran la escalabilidad de la «blockchain» y la velocidad de las transacciones, estas soluciones pueden plantear importantes retos y problemas de opacidad para las fuerzas del orden y los reguladores, debido a la forma en que las redes de Capa 2 operan en relación con las cadenas de bloques subyacentes. Los canales de estado, por ejemplo, como la red Lightning de Bitcoin, implican a dos partes que realizan transacciones de forma privada hasta que cierran el canal y liquidan el saldo en la «blockchain» principal. Todas las transacciones intermedias están ocultas en la «blockchain». Como pueden gestionar sus transacciones fuera de la cadena, estas no se registran inmediatamente en la «blockchain» principal, lo que reduce significativamente la transparencia.

Para mitigar este problema, las agencias policiales deberían asociarse con empresas que se especialicen en análisis de «blockchain», que puedan ayudar a rastrear esas transacciones y comprender cómo interactúan con la «blockchain» subyacente y otras redes.

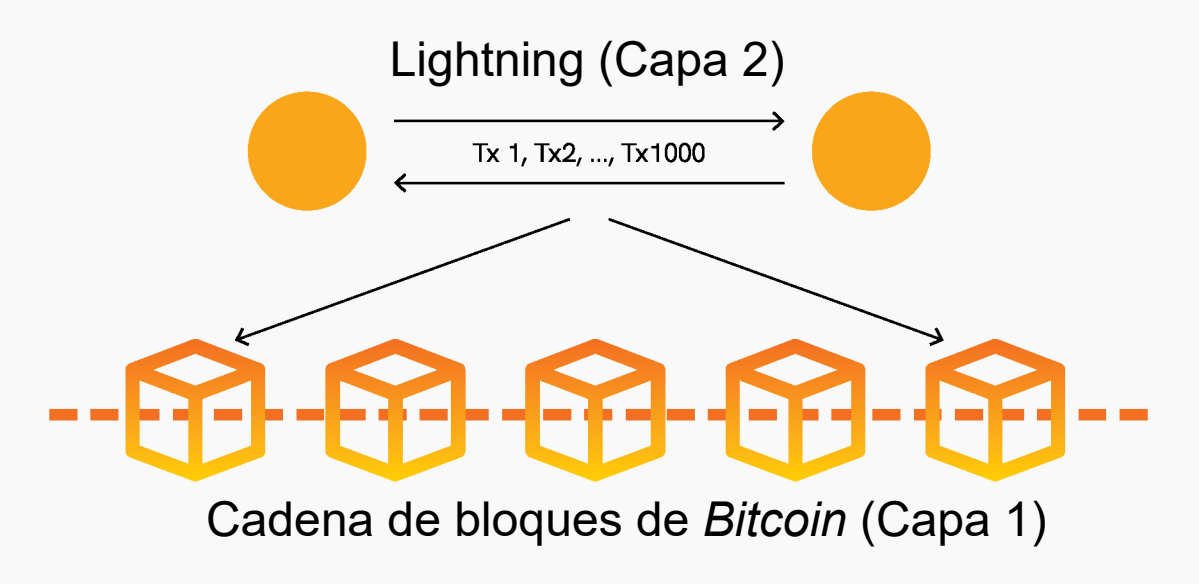


Figura 3 - Representación de la red Lightning de *Bitcoin*

4. Investigación de las criptomonedas

A medida que prolifera el uso de criptomonedas, también lo hacen las actividades ilícitas, desde el blanqueo de capitales y el fraude hasta el tráfico de drogas y la financiación del terrorismo. En respuesta, las fuerzas del orden se enfrentan al enorme desafío de navegar por este ecosistema complejo y descentralizado para defender la justicia y mantener la integridad de los sistemas financieros.

Este capítulo se adentra en el intrincado mundo de las investigaciones sobre criptomonedas, ofreciendo a los y las profesionales de las fuerzas del orden una hoja de ruta integral para navegar con eficacia por los matices de este reino digital.

Navegar por el laberinto de las investigaciones sobre criptomonedas requiere un enfoque polifacético que integre experiencia técnica, perspicacia jurídica y colaboración entre jurisdicciones. Al descifrar la intrincada red de transacciones de «blockchain» e identificar patrones indicativos de actividad ilícita, las fuerzas del orden pueden desmantelar redes delictivas y exigir responsabilidades a los autores.

Además, este capítulo explora la evolución del panorama jurídico en torno a las criptomonedas y su incautación, arrojando luz sobre las tendencias emergentes y los retos normativos.

En última instancia, la lucha contra la delincuencia relacionada con las criptomonedas exige un esfuerzo proactivo y colaborativo, en el que las fuerzas del orden de diferentes jurisdicciones, los VASP y los actores de la industria trabajen conjuntamente para combatir las actividades delictivas relacionadas con los criptoactivos. A través de la educación continua, la innovación y la cooperación, podemos desentrañar las complejidades de las investigaciones de criptomonedas y defender el estado de derecho en la era digital.

4.1. Seguridad de la investigación

Al investigar actividades delictivas que impliquen cualquier uso de Internet, es fundamental buscar y preservar la seguridad y, en algunos casos, el anonimato. Las máquinas virtuales desempeñan un papel crucial en este proceso por varias razones, ya que proporcionan a los investigadores herramientas y funciones valiosas y les

permiten ejecutar un sistema operativo y todas sus aplicaciones en un entorno virtualizado que funciona independientemente de su ordenador físico real.

¿Cuáles son las principales razones para utilizar máquinas virtuales? Hay especialmente dos que son importantes en las investigaciones criminales:

- Aislamiento y contención: permiten a los investigadores crear entornos aislados y contenidos para analizar *software*, archivos, datos o sitios web potencialmente maliciosos o sospechosos. Esto evita la propagación de programas maliciosos («malware») o cualquier efecto perjudicial para el sistema operativo real del investigador y evita que los delincuentes bajo escrutinio localicen e identifiquen a los actores de la investigación;
- Interacción segura con contenido malicioso: En los casos en que los investigadores necesitan interactuar con contenido potencialmente dañino, como correos electrónicos de ataque por suplantación de identidad, sitios web maliciosos o archivos sospechosos, las máquinas virtuales proporcionan un entorno seguro y controlado para hacerlo sin comprometer el sistema real del investigador.

Otro aspecto crucial de este tipo de investigaciones criminales es la preservación de la identidad y ubicación del investigador. Lo que ayuda en esos casos es el uso de una VPN, una red privada virtual, que es una herramienta que permite la comunicación segura y privada a través de Internet. Establece una conexión segura, a menudo denominada túnel, entre su dispositivo (como un ordenador, un teléfono inteligente o una tableta) y un servidor operado por el proveedor de servicios VPN. Este túnel cifra los datos que viajan entre su dispositivo y el servidor, garantizando la confidencialidad e integridad de la información, algo que los investigadores a menudo necesitan cuando se comunican y comparten información delicada.

Además, al enmascarar su dirección IP real con la dirección IP del servidor VPN, una VPN ayuda a anonimizar cualquier actividad en línea. Esto añade una capa de privacidad y es crucial cuando se realizan investigaciones en línea, ya que hace que sea más difícil para los sospechosos o adversarios rastrear a los investigadores hasta sus ubicaciones reales.

¿Debería el investigador utilizar los numerosos servicios VPN gratuitos disponibles en línea o debería optar por la versión basada en suscripción? La elección entre ambos, especialmente en las investigaciones, depende de varios factores, y existen pros y contras asociados a ambas opciones.

Las VPN gratuitas tienen la ventaja obvia de ser gratuitas, lo que puede resultar atractivo para los investigadores que trabajan con limitaciones presupuestarias. También están fácilmente disponibles y los usuarios pueden descargarlas rápidamente y empezar a utilizarlas sin necesidad de pago. Por otro lado, las VPN gratuitas suelen tener limitaciones en cuanto a funciones, ancho de banda y ubicaciones de servidores y pueden comprometer la privacidad del usuario al registrar y vender sus datos a terceros. También pueden experimentar tiempos de inactividad,

tener velocidades de conexión más lentas o carecer de soporte al cliente, lo que afecta a su fiabilidad.

Las VPN de pago ofrecen mejores funciones de seguridad, incluido un cifrado sólido, políticas de no registro y protocolos de seguridad avanzados y, por lo general, ofrecen una mejor infraestructura de servidor, lo que genera conexiones más rápidas y fiables. Esto es crucial para los investigadores que necesitan acceso consistente y seguro a los recursos en línea. Suelen ofrecer asistencia al cliente, lo que puede ser esencial para los investigadores que se encuentren con problemas técnicos o tengan requisitos específicos y es más probable que tengan políticas de privacidad transparentes y un compromiso con la protección de los datos de los usuarios, lo que reduce el riesgo de intercambio de datos no autorizado.

Al investigar a través de Internet, también deben prestar especial atención a no revelar sus direcciones de correo electrónico personales o de trabajo: muchos sitios web requieren autenticación o registro, y una dirección de correo electrónico también se encuentra entre los datos obligatorios solicitados. Por lo tanto, en esas situaciones se puede utilizar una dirección de correo electrónico recién creada.

Los metadatos también son algo que todo investigador debe tener en cuenta si desea permanecer en el anonimato. Los metadatos se refieren a información sobre el archivo en sí, más que al contenido real del mismo. Los metadatos proporcionan información valiosa sobre un archivo, ayudando a los usuarios y a las aplicaciones a organizar, administrar y comprender las características de los datos.

Algunos tipos comunes de metadatos de archivos incluyen el nombre y tipo de archivo, tamaño, fecha y marca de tiempo (incluida la marca de tiempo del último acceso o la última modificación), propietario y permisos. En el caso de imágenes, también se incluiría el modelo del teléfono, la marca y la geolocalización.

4.2. En busca de OSINT

La OSINT (Open Source Intelligence o inteligencia de fuentes abiertas) juega un papel crucial en las investigaciones de criptomonedas: la naturaleza descentralizada, seudónima y global de las criptomonedas hace que los métodos de investigación tradicionales sean menos efectivos, pero la OSINT puede ofrecer datos valiosos para rastrear, localizar y analizar la actividad de «blockchain» y las entidades asociadas. Si bien se pueden usar exploradores de «blockchain» o herramientas profesionales para trazar rutas de transacciones e identificar grupos de direcciones de monederos que controla la misma entidad, las técnicas de OSINT son efectivas para vincular esas direcciones de monederos de criptomonedas a individuos u organizaciones identificables. Los investigadores pueden utilizar datos de foros públicos, plataformas de redes sociales o mercados en línea donde los usuarios podrían haber expuesto sus direcciones de monedero. A continuación, exploraremos algunos de los casos en los que la OSINT resulta crucial en una investigación de criptomonedas.

- **Transparencia de la cadena de bloques:** aunque las transacciones de criptomonedas son seudónimas, el libro mayor de la «blockchain» es público e inmutable. Como veremos más adelante, las técnicas de OSINT se pueden utilizar para rastrear transacciones y analizar patrones en la «blockchain» para vincular direcciones de monedero con entidades del mundo real, utilizando también datos de foros públicos, plataformas de redes sociales o mercados en línea donde los usuarios podrían haber expuesto sus direcciones de monedero.

- **Cuentas de intercambio y datos de KYC:** muchos intercambios de criptomonedas requieren que los usuarios pasen por procesos de conocimiento del cliente (KYC). La OSINT puede ayudar a identificar las bolsas con las que está asociado un monedero, lo que hace posible solicitar datos adicionales de estas bolsas a través de canales legales.

- **Análisis de ataque por suplantación de identidad y ciberestafas:** La OSINT puede identificar patrones y tácticas comunes que se utilizan en estafas relacionadas con criptomonedas, como sitios web de ataque por suplantación de identidad que imitan servicios de criptomonedas legítimos. Al analizar los registros de dominio, el contenido del sitio web y las quejas de los usuarios, los investigadores pueden rastrear estas ciberestafas hasta sus orígenes. Del mismo modo, se pueden utilizar para detectar señales de esquemas Ponzi, fraudes de inversión o sistemas de reactivación y *dumping* en las comunidades de criptomonedas mediante el seguimiento de actividades sospechosas, promociones y picos repentinos en los volúmenes de negociación.

- M**ercados de la red oscura («dark web»):** las actividades delictivas relacionadas con las criptomonedas suelen tener lugar en la red oscura («dark web»). Las técnicas de OSINT permiten a los investigadores supervisar estos mercados y foros para rastrear transacciones ilícitas, esquemas de blanqueo de capitales o incluso pagos de rescates.

- **Inteligencia de redes sociales:** los usuarios a menudo comparten direcciones de criptomonedas en plataformas de redes sociales, ya sea consciente o inconscientemente, lo que puede ser crucial para vincular cuentas a identidades del mundo real. Los investigadores buscarán debates sobre transacciones de criptomonedas que estén relacionadas con ciberestafas, fraudes o piratería.

4.3. Técnicas de investigación

Aunque hemos visto que el uso de criptomonedas proporciona a los delincuentes un cierto nivel de anonimato y puede frustrar a los investigadores que intentan localizar los productos del delito o descubrir el origen de determinadas transacciones, existen técnicas que pueden ayudar a las fuerzas del orden a utilizar datos de «blockchain» y otros indicios para traspasar el velo del anonimato.

Como en las investigaciones a la antigua usanza, las compras encubiertas simuladas siguen constituyendo un método útil. Tanto si se trata de un mercado de la red oscura

(«dark web») como de cualquier otro servicio que acepte criptomonedas, una compra controlada expondrá al menos una dirección bajo el control de los delincuentes: para recibir fondos, se debe proporcionar al comprador al menos una dirección de recepción y ese sería el punto de partida de la investigación.

Las técnicas de indagación se pueden aplicar para crear un grupo de direcciones que estén bajo el control del mismo sospechoso. Una vez identificado un clúster, el trabajo de los investigadores consistirá en seguir esas transacciones, en ambas direcciones (transacciones que envían monedas al clúster objetivo, pero también enviadas desde el clúster) hasta encontrar una dirección que esté controlada por una entidad que pueda proporcionar pistas sobre la identidad del receptor (o remitente) de esas transacciones.

Entre las técnicas de indagación más comunes podemos encontrar:

- **Entrada múltiple o propiedad de entrada común:** es una de las principales técnicas de indagación utilizadas por las empresas de análisis de cadenas para determinar el propietario de UTXO específicas. Esta técnica de indagación actualmente supone que todas las entradas de una transacción determinada pertenecen al mismo propietario. Esta técnica de indagación nunca ha ofrecido certeza y, a medida que *Bitcoin* continúa evolucionando, se está volviendo menos fiable. Tecnologías como CoinJoin, CoinSwap, las transacciones *multisig* regulares y, en el futuro, las transacciones MuSig contradicen esta heurística al aceptar aportaciones de muchas partes diferentes.

- **Detección de cambio de dirección:** la heurística de detección de cambio de dirección se basa en los atributos de UTXO. Dado que enviar la cantidad exacta de fondos especificada al receptor es todo un reto, los fondos excedentarios generalmente se devuelven al remitente a través de una dirección de cambio. Por lo tanto, detectar direcciones de cambio es esencial ya que forman parte integrante de las operaciones de la entidad.

Mientras siguen y rastrean transacciones en la «blockchain», los investigadores deben tener en mente sus objetivos finales: identificar a los sospechosos, cuando aún no los conozcan, y asegurar sus condenas, pero también, y este aspecto es cada vez más importante, localizar e incautar sus activos.

Existen herramientas gratuitas que permiten a los investigadores navegar por la «blockchain» y seguir el rastro del dinero. Arkham es una de esas herramientas que permiten tener una visión rápida de diferentes cadenas de bloques y seguir las transacciones de una dirección a otra. A menudo se aplica una agrupación básica que permite la detección de transferencias a los VASP. Sin embargo, lo que les suele faltar es una visualización adecuada y una fuente verificable de la información utilizada para agrupar direcciones.

4.4. Herramientas de análisis de cadenas de bloques

Por otro lado, las fuerzas del orden utilizan cada vez más herramientas de proveedores de análisis de «blockchain» que proporcionan una forma integral, potente y fiable de extraer información. Las herramientas de análisis de cadena de bloques ofrecen visibilidad de las transacciones de «blockchain». La información registrada en la «blockchain» se codifica y verifica en registros inmutables y de acceso público. Estas herramientas supervisan estos registros y estructuran los datos para ilustrar las conexiones entre varios monederos de criptomonedas.

¿Qué hace que una herramienta de análisis de «blockchain» sea buena?

- **Cobertura:** las herramientas deben poder analizar y rastrear una amplia cartera de activos digitales y cadenas de bloques.
- **Interfaz de usuario:** una interfaz intuitiva y fácil de usar facilita el análisis de las transacciones y hace que sea intuitivo seguirlas e identificar entidades.
- **Información actualizada:** las herramientas necesitan supervisar las transacciones en diferentes cadenas de bloques en tiempo real. También deben estar actualizadas según las últimas listas de sanciones.
- **Gestión de casos:** las herramientas proporcionarán a los investigadores una manera sencilla de compartir información, análisis y gráficos, tanto interna como externamente.
- **Fuente de información transparente y fiable:** la herramienta de análisis debe proporcionar la información que los llevó a realizar una atribución particular de propiedad, ya que esta información puede verificarse por duplicado, respaldarse con otras fuentes y será fundamental ante un tribunal.
- **Herramientas de visualización:** los gráficos facilitan la comprensión de la actividad en la «blockchain» y las interacciones entre direcciones, y aportan pruebas ante los tribunales que ilustrarán claramente los pasos dados por los delincuentes.

Al utilizar esas herramientas, los investigadores normalmente seguirán los fondos en la «blockchain», moviéndose de una dirección a otra, y a veces de una «blockchain» a otra, hasta que se conozca e identifique su ubicación. Aquí se enfrentarán a dos escenarios posibles: o bien los fondos se mantienen en monederos privados o no alojados, o bien han llegado a un VASP o un servicio similar, con el objetivo de ser convertidos a fiat y cobrados. Dependiendo de la solución que hayan utilizado los delincuentes, los investigadores adaptarán sus estrategias de investigación en consecuencia.

11. https://platform.arkhamintelligence.com

4.5. Monederos (privados) no alojados

Al seguir transacciones en la «blockchain», a menudo los investigadores se enfrentan a esta situación: después de una serie de saltos (un salto se refiere a una transacción que mueve fondos de una dirección a la siguiente), los fondos llegan a una dirección y no se mueven más. Algunas herramientas los visualizarán como “no gastados” o “liquidados”: el resultado es el mismo, los fondos se encuentran en una dirección que parece, según las herramientas utilizadas, privada; los fondos no se han depositado en una bolsa ni en ningún otro servicio que pueda ser citado. Y lo que es más importante para las investigaciones una el sospechoso es quien posee las claves privadas.

Un monedero no alojado a menudo se denomina almacenamiento en frío o autocustodia y permite a los usuarios administrar el saldo de sus criptomonedas independientemente de una plataforma, de manera similar a mantener efectivo en un monedero personal. Algunos ejemplos son los monederos de *hardware* como Ledger o Trezor, aplicaciones móviles o soluciones de *software* como Electrum. Por el contrario, un monedero alojado es administrado por una plataforma de terceros, como plataformas verificadas como Coinbase, Crypto.com o Binance.

En esta situación, para incautar los productos del delito y los fondos vinculados a la actividad ilícita, los investigadores deberán localizar las claves privadas y tenerlas bajo control, antes de avanzar al siguiente paso.

> Una clave privada tiene el siguiente aspecto:
>
> **KxRpTxdFnmanomZzq8YVt5NcfJQbi19xDTDkmLV1D8fHEKFyqBmT** (Bitcoin)
>
> **2410FD14C3AA9340E57FE64B25CDCDE514A85CB1B46E157E11B3232264254373** (Bitcoin - hexadecimal)
>
> **DC38EE117CAE37750EB1ECC5CFD3DE8E85963B481B93E732C5D0CB66EE6B0C9D** *(Ethereum - hexadecimal)*

Una clave privada es, esencialmente, una larga cadena de números y letras: puede almacenarse, por lo tanto, en numerosos lugares diferentes, tanto físicos como digitales. En los siguientes ejemplos, consideraremos diferentes escenarios y, para cada uno de ellos, localizaremos las claves privadas.

Aplicaciones móviles

La tipología más común de autocustodia es un monedero móvil, una aplicación de *software* instalada en un teléfono o tableta que permite a los usuarios recibir, enviar y almacenar criptomonedas.

Existen dos tipos principales de monederos de criptomonedas: con custodia y sin custodia. Los monederos con custodia son administrados por un tercero que guarda

y protege sus claves privadas en su nombre. Estos terceros a menudo proporcionan sistemas de seguridad de datos robustos y de nivel empresarial para proteger sus activos, de manera análoga a cómo las empresas protegen su información sensible. Muchas bolsas de criptomonedas, como Coinbase o Binance, ofrecen monederos con custodia a sus usuarios, lo que garantiza que sus fondos se almacenen con medidas de seguridad avanzadas.

Por el contrario, los monederos no custodiados le dan control y responsabilidad total sobre sus claves privadas. Esto significa que usted es el único responsable de la seguridad y la gestión de su criptomoneda. Las monederos no custodiados generalmente se utilizan en dispositivos personales, como teléfonos inteligentes u ordenadores. El uso de un monedero no custodiado proporciona a una persona acceso directo a los fondos sin depender de un tercero.

En esta situación, una vez que se encuentra un *software/*aplicación similar, los investigadores pueden iniciar una transacción directamente desde él, moviendo los fondos a una dirección controlada.

Monederos de *hardware*

Un monedero de *hardware* es un dispositivo físico diseñado para almacenar de forma segura las claves privadas. A diferencia de los monederos de *software* vistos anteriormente, los monederos de *hardware* ofrecen una capa adicional de seguridad al mantener las claves privadas fuera de línea, lo que reduce el riesgo de que queden expuestas a un programa malicioso o a piratas informáticos.

Las características principales de los monederos de *hardware* incluyen:

1. **Memoria autónoma («offline»):** Las claves privadas se almacenan en el propio dispositivo y nunca salen de él, incluso cuando está conectado a un ordenador o dispositivo móvil. Esto garantiza que sus claves permanezcan seguras incluso si su ordenador se ve comprometido.

2. **Transacciones seguras:** Cuando uno necesita enviar o recibir criptomonedas, la transacción se firma dentro del propio monedero de *hardware*. Esto significa que las claves privadas nunca estarán expuestas a su dispositivo conectado ni a Internet.

3. **Protección con PIN:** Los monederos de *hardware* generalmente están protegidos por un código PIN, lo que añade una capa adicional de seguridad. Incluso en el caso de pérdida o robo del dispositivo, el PIN ayuda a prevenir el acceso no autorizado.

4. **Copia de seguridad y recuperación:** Los monederos de *hardware* generalmente vienen con una frase semilla de recuperación, una lista de palabras que se pueden usar para restaurar el monedero (véase el siguiente párrafo).

5. **Compatibilidad:** La mayoría de los monederos de *hardware* son compatibles con varias criptomonedas y se pueden usar con múltiples aplicaciones de monedero, lo que aporta flexibilidad a la gestión de diferentes activos digitales.

Algunos ejemplos populares de monederos de *hardware* son Ledger y Trezor. Los investigadores, en primer lugar, necesitarían obtener físicamente el monedero de *hardware*. Esto suele ocurrir mediante órdenes de registro o redadas: las fuerzas del orden pueden ejecutar órdenes de registro para incautar monederos de *hardware* físicos de la propiedad de un sospechoso.

Como en el ejemplo anterior de monederos móviles, en esta situación los investigadores pueden incautar el monedero e iniciar una transacción desde el mismo para mover los fondos a un monedero controlado. Una vez que el monedero de *hardware* está bajo custodia, para acceder a los fondos se requiere el uso, si esta función está habilitada, del PIN o la frase de contraseña del dispositivo: las autoridades podrían obligar al propietario a proporcionar el PIN o la frase de contraseña a través de medios legales, como órdenes judiciales o negociaciones de declaraciones de admisión de culpabilidad.

Frases semilla

Tanto si los sospechosos han utilizado un monedero móvil como uno de *hardware*, tienen una característica importante en común: ambos utilizan una forma de protección, llamada “frase semilla”.

Una frase semilla, también conocida como frase de recuperación o frase mnemotécnica, es una secuencia de palabras generadas por un monedero de criptomonedas que da acceso al usuario a los fondos del monedero. Sirve como mecanismo de respaldo, permitiendo al usuario recuperar su monedero y su contenido en caso de pérdida, daño o inaccesibilidad.

Normalmente, una frase semilla consta de 12, 18 o 24 palabras generadas aleatoriamente. Estas palabras se seleccionan de una lista estandarizada (como la lista de palabras BIP-39) para garantizar la uniformidad y la compatibilidad entre diferentes monederos. El uso de palabras comunes en lugar de cadenas complejas de caracteres facilita a los usuarios escribir y almacenar la frase de forma segura. Cuando se crea un nuevo monedero, su *software* genera una frase semilla e indica al usuario que la escriba y la guarde de forma segura. Esta frase semilla está vinculada a la clave privada del monedero a través de un algoritmo determinista, lo que permite la regeneración de las claves privadas a partir de la frase semilla.

Incluso si no se encuentra un monedero durante un registro del sospechoso, la recuperación de la frase semilla es suficiente para tomar el control de los activos y moverlos a una dirección controlada. Los investigadores crearán un nuevo monedero, o usarán uno que ya tengan en su poder y, a continuación, introducirán la frase semilla en el *software* del monedero. El software utiliza la frase para regenerar las claves

privadas y las direcciones asociadas, dando a los investigadores acceso a sus tenencias de criptomonedas.

Pasos que hay que seguir:

- Descargue el *software* del monedero u obtenga un nuevo monedero de *hardware*.
- Durante el proceso de configuración, elija la opción de restaurar un monedero.
- Introduzca la frase inicial con precisión cuando se le solicite.
- El *software* del monedero regenerará las claves y direcciones privadas, dándole acceso a sus fondos

Planificar con antelación la captura de un monedero no alojado

A medida que las fuerzas del orden se preparan para un registro e incautación de monederos no alojados (como monederos de *hardware* o *software*), es esencial abordar la operación con una planificación meticulosa y el cumplimiento de los protocolos legales. Debido a las peculiaridades de la incautación de criptomonedas, la operación debe planificarse con antelación para asegurarse de que todos los puntos siguientes se tengan en cuenta y se incluyan adecuadamente.

Obtenga las órdenes judiciales adecuadas: Obtenga una orden de registro que autorice explícitamente la incautación de activos digitales, incluidos monederos de *hardware*, monederos de *software* y cualquier dispositivo relacionado. Asegúrese de que la orden detalle los lugares específicos que se van a registrar y los tipos de artículos que se van a incautar para evitar sobrepasar los límites legales.

Consulte a los expertos: Recurra a expertos en ciberseguridad y criptomonedas para comprender los aspectos técnicos de los monederos no alojados y cómo se puede acceder a ellos o incautarlos.

Planificación operativa: Recurra a la vigilancia y a informantes para recopilar información sobre las propiedades del sospechoso y los posibles escondites de los monederos de *hardware*. Analice la huella digital del sospechoso, incluidas las redes sociales, las transacciones en línea y las comunicaciones, para identificar posibles ubicaciones de los activos digitales.

Prepare el equipo especializado: Dote al equipo de herramientas forenses diseñadas para gestionar y analizar monederos de *hardware* y dispositivos cifrados. Tenga preparadas herramientas de recuperación de datos para extraer información de los dispositivos incautados. Asegúrese de contar con personal de soporte técnico disponible para que proporcione asistencia con cualquier problema técnico inesperado durante la operación.

Ejecución del registro: Asegure la zona para evitar que el sospechoso destruya u oculte dispositivos durante el registro y actúe con rapidez para evitar que use

mecanismos de autodestrucción o herramientas de cifrado para borrar datos. Recoja todos los dispositivos que puedan almacenar o tener acceso a activos digitales, incluidos ordenadores, teléfonos inteligentes, tabletas, unidades USB y notas escritas que puedan contener frases semilla.

Manipule los dispositivos con cuidado: manipule todos los dispositivos con cuidado para evitar la destrucción de datos. En el caso de los monederos de *hardware*, asegúrese de que permanezcan apagados para evitar cualquier comando de borrado remoto. Registre la ubicación y el estado de cada artículo incautado, incluidos los números de serie y cualquier identificador visible.

4.6. Monederos alojados

Un monedero alojado, también conocido como monedero con custodia, es un tipo de monedero de criptomonedas donde un tercero (como una plataforma de criptomonedas o un proveedor de servicios de monedero) custodia y administra las claves privadas del usuario en su nombre. Este tercero es responsable de proteger los fondos y prestar diversos servicios relacionados con la gestión y las transacciones del monedero.

La mayoría de los proveedores de monederos alojados realizan procedimientos de conocimiento del cliente (KYC) como parte de sus esfuerzos de cumplimiento de la normativa. El KYC es un proceso utilizado por las instituciones financieras, incluidas las plataformas de criptomonedas y los proveedores de monederos, para verificar la identidad de sus clientes y evaluar el riesgo de actividades ilegales, como el blanqueo de capitales y la financiación del terrorismo. En esta fase, se pide a los usuarios que proporcionen información personal, como su nombre completo, fecha de nacimiento, dirección, datos bancarios, documentos de identificación emitidos por el Gobierno (p. ej., pasaporte, permiso de conducir) y lugar de residencia.

Suele ser una buena noticia cuando, al seguir transacciones en la «blockchain», los investigadores ven que los fondos se colocan en una dirección controlada por un proveedor de servicios como un VASP: se refiere a que ahora los investigadores pueden, a través de los mecanismos apropiados, obtener información del servicio sobre la identidad de la persona que controla la cuenta y solicitar al servicio que congele los criptoactivos (o moneda fiat) mantenidos a nombre del cliente.

Es fundamental que el investigador entienda que, una vez que ve en la «blockchain» una transacción que llega a un servicio como un VASP, debe dejar de seguir la cadena de transacciones posteriores. Cuando los usuarios depositan criptomonedas en un servicio, se les proporcionará una dirección de depósito, es decir, la dirección criptográfica a la que pueden enviar dinero para acreditarlo en su cuenta. Después de acreditar al usuario la cantidad correspondiente, los servicios generalmente moverán esos fondos a otros monederos internos y los destinarán a otras operaciones que no tienen nada que ver con el depósito de dinero por parte del usuario. Siempre y cuando, en una etapa posterior, los usuarios deseen mover y retirar los fondos que han depositado, por ejemplo, a un monedero no alojado o a otro proveedor, los fondos

provendrán de una dirección completamente ajena y diferente de la dirección de depósito utilizada inicialmente. La única forma de comprender las transacciones internas y determinar qué dirección se ha utilizado para retirar fondos (y, en consecuencia, determinar la dirección de recepción) es recibir esta información del proveedor de servicios.

¿Qué tipo de información puede proporcionar el proveedor de servicios a las solicitudes de las fuerzas del orden?

- **Dirección de depósito del usuario:** se trata de la dirección asignada al usuario para depositar criptoactivos. Esta dirección puede seguir siendo la misma, incluso en caso de múltiples depósitos, o cambiar con el tiempo.
- **Dirección de retirada del usuario:** si los criptoactivos se trasladan del VASP a un monedero alojado internamente, a un servicio u otro VASP, esta información puede ponerse a disposición de los investigadores.
- **KYC:** todos los datos relacionados con el cliente, incluyendo nombre completo, fecha de nacimiento, dirección, documentos de identificación emitidos por el Gobierno, lugar de residencia y datos bancarios. Si el cliente es una persona jurídica, estos datos incluirán los documentos de constitución.
- **2FA:** 2FA corresponde a las siglas de Two-Factor Authentication (autenticación de dos factores o en dos fases). Se trata de una medida de seguridad que se utiliza para agregar una capa adicional de protección a las cuentas y servicios en línea. El segundo factor es algo que posee el usuario, como un dispositivo móvil, un *token* de seguridad o una clave de *hardware.* Esto puede proporcionar a los investigadores un número de teléfono móvil utilizado por el sospechoso.

Una citación a un VASP funciona de manera similar a una citación emitida a cualquier otra institución financiera o proveedor de servicios. Sin embargo, las fuerzas del orden deben tener en cuenta algunos aspectos antes de presentar una solicitud.

- **Lenguaje correcto:** la criptoesfera ha desarrollado su propio conjunto de jerga y terminología específicas a lo largo de los años. Esta jerga es utilizada a menudo por entusiastas de las criptomonedas, comerciantes, desarrolladores y otros participantes en el ecosistema criptográfico, pero también se ha generalizado y puede ser muy específica. Redactar una citación a un proveedor de servicios requerirá que el investigador se familiarice con la terminología utilizada, o incurrirá en el riesgo de que la solicitud no se comprenda completa y cabalmente.
- **Uso de archivos de texto:** como hemos visto antes, las direcciones, claves privadas e identificadores de transacciones son largas cadenas de números y letras, propensas a errores y erratas si uno tiene que leer y teclear desde un documento PDF. Es una buena práctica enviar esta información en un formato de archivo que permita copiar y pegar, como archivos doc o txt.

- **Contactos informales:** En los últimos años, los VASP han ampliado sus equipos dedicados a ayudar a las fuerzas del orden con sus solicitudes. Además, algunas actuaciones son sensibles al tiempo y requieren acciones inmediatas. Establecer contactos informales con los VASP, incluso antes de que se presente una solicitud formal, ayuda a acelerar el proceso de varias maneras: se puede revisar un borrador de la solicitud y modificarlo si es necesario, evitando así largas idas y venidas; los VASP pueden evaluar si se ha proporcionado toda la información requerida; en ocasiones en las que el tiempo apremia, los VASP pueden adoptar medidas urgentes, como impedir cualquier transacción desde la cuenta bajo escrutinio, a la espera de la citación formal.

5. Cooperación internacional

A medida que los delincuentes operan cada vez más a través de las fronteras, aprovechando el alcance global de la tecnología de «blockchain», la necesidad de cooperación internacional en las investigaciones criminales de criptomonedas nunca ha sido más crítica. Las fuerzas del orden deben explorar las complejidades del rastreo de transacciones ilícitas que abarcan múltiples jurisdicciones y destacar los mecanismos y marcos esenciales que facilitan la cooperación transfronteriza entre las fuerzas del orden, los organismos reguladores y las instituciones financieras.

A diferencia de los sistemas financieros tradicionales, que a menudo están regulados y supervisados en el marco de jurisdicciones específicas, la naturaleza descentralizada y seudónima de las criptomonedas permite a los perpetradores de delitos ocultar sus identidades y ubicaciones de manera efectiva.

Varias tipologías de actividades delictivas que involucran criptomonedas son de naturaleza especialmente transnacional, entre ellas:

- **Blanqueo de capitales:** Los delincuentes utilizan criptomonedas para blanquear dinero mediante la conversión de fondos ilícitos en activos digitales, que luego pueden trasladarse a través de las fronteras e intercambiarse por moneda fiat en diferentes jurisdicciones, lo que hace que los fondos sean más difíciles de rastrear.
- **Fraudes y estafas:** Los esquemas fraudulentos como los esquemas Ponzi, los ataques por suplantación de identidad y las estafas de inversión pueden dirigirse a víctimas en varios países simultáneamente, aprovechando el anonimato de las transacciones de criptomonedas para eludir la detección y el enjuiciamiento.
- **Ataques de programas de secuestro:** Los ciberdelincuentes implementan programas de secuestro para bloquear los datos de las víctimas y exigir el pago en criptomonedas. Estos ataques suelen orquestarse desde un país, se dirigen a entidades de otro y encauzan los pagos a través de varios intercambios internacionales para ocultar el rastro del dinero.
- **Financiación del terrorismo:** Las organizaciones terroristas han recurrido cada vez más a las criptomonedas para financiar sus actividades, aprovechando la

capacidad de transferir valor a través de las fronteras sin la supervisión típica de los sistemas bancarios tradicionales.

Uno de los retos más importantes en la lucha contra los delitos transnacionales relacionados con las criptomonedas es la cuestión de la jurisdicción. Las fuerzas del orden normalmente se limitan a operar en el ámbito de sus fronteras nacionales, mientras que las transacciones de criptomonedas pueden cruzar fácilmente estas fronteras sin ninguna presencia física. Esta desconexión crea varios problemas:

- **Solapamiento jurisdiccional:** Varios países pueden reclamar jurisdicción sobre un solo delito relacionado con criptomonedas, lo que genera conflictos e ineficiencias en la investigación y el enjuiciamiento.
- **Falta de jurisdicción:** En algunos casos, puede que ningún país tenga una jurisdicción clara, especialmente si el delincuente y la víctima se encuentran en países diferentes y los servidores o intercambios utilizados están ubicados en otro conjunto de jurisdicciones.
- **Incoherencias jurídicas:**
  Las leyes y normativas sobre criptomonedas varían de un país a otro, lo que genera incoherencias en la definición, investigación y enjuiciamiento de los delitos. Esto puede crear lagunas que los delincuentes aprovechan para eludir la justicia.

5.1. Mecanismos de cooperación internacional

La cooperación internacional en las investigaciones penales sobre criptomonedas se basa en una serie de mecanismos diseñados para facilitar la colaboración eficaz entre las naciones. Estos mecanismos permiten el intercambio de información, recursos y experiencia, lo que hace posible abordar los delitos complejos y transnacionales relacionados con las criptomonedas de manera más eficiente.

Tratados de Asistencia Jurídica Mutua

Los tratados de asistencia jurídica mutua (los MLAT) son acuerdos bilaterales o multilaterales entre países que proporcionan un marco para solicitar e intercambiar pruebas en investigaciones criminales y procesos penales. Los tratados de asistencia jurídica mutua son cruciales para obtener información que está fuera del alcance de las fuerzas del orden nacionales.

- **Proceso:** Cuando un país necesita asistencia de otra jurisdicción, presenta una solicitud de asistencia jurídica mutua a través de las autoridades centrales designadas, normalmente el Ministerio de Justicia o una entidad similar. La solicitud describe la naturaleza de la investigación, la asistencia específica requerida y la base jurídica de la solicitud.

- **Ventajas:** Los tratados de asistencia jurídica mutua facilitan la obtención de pruebas, como registros de transacciones de plataformas de criptomonedas extranjeras, declaraciones de testigos y análisis forenses digitales. Garantizan que las pruebas se obtengan legalmente y puedan ser admisibles en los tribunales.

- **Aplicación:** En un caso de gran repercusión, un país de América del Sur podría usar un tratado de asistencia jurídica mutua para solicitar datos de transacciones a una bolsa de criptomonedas europea con el fin de rastrear fondos vinculados a un ataque de «ransomware». Esta cooperación es esencial para construir un caso sólido contra los perpetradores de delitos.

Equipos conjuntos de investigación (ECI)

Los ECI son grupos de colaboración formados por las fuerzas del orden de varios países para trabajar en casos específicos relacionados con la delincuencia transnacional. Los ECI permiten compartir información en tiempo real y realizar acciones coordinadas.

- **Proceso:** Los países implicados en una investigación transnacional acuerdan establecer un ECI mediante un convenio formal. Los miembros del ECI, entre los que puede haber policías, fiscales y otros especialistas, trabajan juntos, a menudo en un mismo lugar, para poner en común sus recursos y pericia.

- **Ventajas:** Los ECI mejoran la eficiencia operativa, reducen la duplicación de esfuerzos y permiten acciones sincronizadas, como detenciones y registros simultáneos en diferentes países. Fomentan la confianza y la estrecha cooperación entre socios internacionales.

- **Aplicación:** Podría formarse un ECI entre organismos de los Estados Unidos, el Reino Unido y Australia para investigar una trama mundial de fraude con criptomonedas. Al trabajar en conjunto, el equipo puede compartir información de inteligencia rápidamente, coordinar los interrogatorios de sospechosos y testigos, y realizar redadas simultáneas para desmantelar la red delictiva.

Plataformas de intercambio de información

Las plataformas de intercambio de información, como el Grupo Egmont y la aplicación de red de intercambio seguro de información (SIENA) de Europol, facilitan el intercambio rápido de información de inteligencia y datos entre países.

- **Proceso:** Los organismos participantes comparten información a través de canales seguros y normalizados. Estas plataformas proporcionan un marco para presentar y responder a las solicitudes de información, garantizando la integridad y confidencialidad de los datos.

- **Ventajas:** Las plataformas de intercambio de información permiten el acceso oportuno a datos críticos, como los informes sobre transacciones sospechosas, que pueden ser fundamentales para identificar y desbaratar actividades delictivas. También son compatibles con herramientas analíticas que ayudan a rastrear transacciones de criptomonedas y a descubrir redes delictivas.

- **Aplicación:** A través del Grupo Egmont, una unidad de inteligencia financiera (UIF) de Canadá podría alertar a sus homólogas de Japón y Alemania sobre transacciones sospechosas de criptomonedas vinculadas a una operación de blanqueo de capitales. Este rápido intercambio de información permite una respuesta coordinada y la congelación de activos ilícitos.

INTERPOL y Europol

Las organizaciones policiales internacionales como INTERPOL y Europol desempeñan un papel vital en el fomento de la cooperación internacional en las investigaciones sobre criptomonedas.

- **Proceso:** INTERPOL y Europol proporcionan plataformas para que las fuerzas del orden colaboren en las investigaciones, compartan información de inteligencia y accedan a recursos especializados. También organizan sesiones de formación, conferencias y operaciones conjuntas.

- **Ventajas:** Estas organizaciones mejoran las capacidades de las fuerzas del orden a nivel mundial al ofrecer experiencia en investigación forense digital, ciberseguridad y rastreo de criptomonedas. También facilitan las investigaciones transfronterizas mediante la coordinación y el apoyo.

- **Aplicación:** El Centro Europeo de Ciberdelincuencias (EC3) de Europol podría liderar un esfuerzo coordinado en el que participen múltiples fuerzas del orden para desmantelar un mercado de la red oscura («dark web») que comercializa mercancías y servicios ilegales pagados con criptomonedas. INTERPOL puede emitir alertas internacionales, como notificaciones rojas, para localizar y detener a sospechosos en todo el mundo.

5.2. Retos y obstáculos en la cooperación internacional

A pesar de los marcos y mecanismos existentes para facilitar la cooperación internacional en las investigaciones penales sobre criptomonedas, siguen persistiendo numerosos retos y obstáculos. Estas barreras pueden dificultar significativamente la eficacia de los esfuerzos transfronterizos para combatir los delitos relacionados con las criptomonedas.

Uno de los principales retos en la cooperación internacional es la cuestión de los conflictos jurisdiccionales. Los distintos países tienen diferentes sistemas jurídicos,

leyes y reglamentos relativos a las criptomonedas, lo que puede generar conflictos y complicaciones en las investigaciones y los enjuiciamientos. Por ejemplo, un defraudador de criptomonedas que opera desde un país, busca víctimas en otro y utiliza una bolsa en un tercer país para blanquear los productos del delito puede crear un escenario complejo en el que la determinación de la jurisdicción se convierta en contenciosa. El desarrollo de convenios y marcos internacionales que definan claramente los límites jurisdiccionales y los protocolos de resolución de conflictos puede ayudar a mitigar estos problemas.

Además, la falta de uniformidad en los enfoques jurídicos y reglamentarios de las criptomonedas en las distintas jurisdicciones plantea importantes retos para la cooperación internacional. Los países tienen diferentes definiciones de lo que constituye un delito relacionado con criptomonedas, distintas normativas de pruebas y regulaciones dispares para las bolsas de criptomonedas y las instituciones financieras. Estas incoherencias pueden crear lagunas jurídicas que los delincuentes aprovechan para eludir la acción de la justicia. Por ejemplo, operar una plataforma de criptomonedas no registrada podría ser un delito penal en un país, mientras que en otro solo puede dar lugar a una multa. Promover la armonización internacional de las regulaciones sobre criptomonedas y adoptar normas mundiales, como las recomendadas por el GAFI, puede contribuir a crear un entorno jurídico más cohesionado.

Por último, la rápida evolución de la tecnología de las criptomonedas plantea un reto importante, ya que las fuerzas del orden en todo el mundo a menudo tienen dificultades para mantenerse al día de los últimos avances y técnicas que utilizan los delincuentes. Las disparidades tecnológicas y los distintos niveles de experiencia entre los países dan lugar a capacidades de aplicación de la ley desiguales. Algunos países pueden carecer de las herramientas, los recursos o el personal formado necesarios para investigar y procesar eficazmente los delitos relacionados con las criptomonedas. Por ejemplo, un país con una infraestructura y conocimientos tecnológicos limitados puede ser incapaz de rastrear transacciones sofisticadas de criptomonedas o de recuperar pruebas digitales, lo que obstaculiza la investigación en general. Mejorar la colaboración internacional en iniciativas de desarrollo de capacidades, incluidos programas de formación, asistencia técnica e intercambio de recursos, puede ayudar a solventar estar carencias. El establecimiento de centros internacionales de excelencia en materia de ciberseguridad y análisis forense de criptomonedas puede proporcionar apoyo continuo y difusión de conocimientos.

6. Recomendaciones

Las recomendaciones proporcionan un marco detallado de estrategias y mejores prácticas destinadas a abordar el uso indebido de criptoactivos y servicios relacionados. Se centran en la prevención de la explotación de monedas digitales con fines delictivos, incluida la creación, ocultación y blanqueo de fondos ilegales. Mediante el establecimiento de directrices claras, estas Recomendaciones guían a las organizaciones y autoridades en la implementación de medidas sólidas para detectar, rastrear e interrumpir actividades financieras ilícitas dentro del ecosistema de las criptomonedas.

Obtener las herramientas adecuadas:

El espacio criptográfico está avanzando rápidamente, junto con las estrategias utilizadas por los delincuentes. Como consecuencia de ello, los investigadores se enfrentan a mayores retos a la hora de rastrear criptoactivos ilícitos. Además, el auge de las plataformas de finanzas descentralizadas (DeFi) y los contratos inteligentes presenta obstáculos más significativos. Las herramientas de análisis de cadena de bloques son cruciales para las fuerzas del orden porque permiten el seguimiento, rastreo y análisis de las transacciones de criptomonedas, convirtiendo la transparencia de la tecnología de «blockchain» en una poderosa herramienta de lucha contra la delincuencia. Estas herramientas ayudan a vincular direcciones de monederos sospechosas con identidades del mundo real, detectar técnicas de blanqueo de capitales e identificar patrones de fraude, incluso en entornos de finanzas descentralizadas (DeFi). También apoyan las investigaciones sobre programas de secuestros, proporcionan pruebas admisibles en procedimientos judiciales y mejoran la colaboración entre organismos internacionales e instituciones financieras. Al automatizar los procesos de investigación y adaptarse a los métodos de ofuscación en evolución, las herramientas de análisis de «blockchain» permiten a las fuerzas del orden responder de manera efectiva a la naturaleza dinámica de los delitos relacionados con las criptomonedas.

Ampliar conocimientos a través de la formación:

La formación es vital para las fuerzas del orden en las investigaciones de delitos criptográficos porque desarrolla el conocimiento y las habilidades necesarias para gestionar las complejidades de la tecnología de «blockchain» y las tácticas delictivas en evolución. Proporciona a los agentes una comprensión sólida de cómo funcionan las criptomonedas y de cómo utilizar herramientas de análisis de «blockchain» especializadas para rastrear transacciones ilícitas y vincularlas con identidades del mundo real. A medida que los delitos relacionados con las criptomonedas evolucionan con nuevas innovaciones como las finanzas descentralizadas (DeFi), los mezcladores y las «privacy coins», la formación garantiza que los investigadores se mantengan al día de los últimos métodos que utilizan los delincuentes para ocultar sus huellas. La formación también hace hincapié en el cumplimiento de la legalidad, enseñando a los agentes a gestionar las pruebas digitales adecuadamente para que sigan siendo admisibles en los tribunales, fortaleciendo así su capacidad para construir casos jurídicos sólidos. Además, los agentes bien formados pueden llevar a cabo investigaciones de manera más eficaz, reduciendo los errores y aumentando la velocidad y precisión de su trabajo. La formación promueve una mejor colaboración entre las fuerzas del orden, tanto a nivel nacional como internacional, lo que permite un intercambio eficaz de información en la lucha mundial contra los delitos criptográficos. En última instancia, la formación continua es crucial para permitir que las fuerzas del orden sigan el ritmo del cambiante panorama de las criptomonedas, se adapten a los nuevos retos y prevengan y procesen con éxito los delitos financieros digitales.

Aumentar la cooperación:

La colaboración entre organismos nacionales e internacionales es crucial para la eficacia de las investigaciones sobre delitos criptográficos, ya que estas a menudo abarcan múltiples jurisdicciones y requieren coordinación entre diferentes áreas de especialización. Los organismos nacionales, como las unidades de inteligencia financiera, desempeñan un papel clave al proporcionar información de inteligencia clara y procesable basada en datos de los proveedores de servicios de activos virtuales. Los investigadores y fiscales también pueden confiar en las agencias de recuperación de activos para garantizar que las pruebas digitales, como el acceso a las claves privadas de criptomonedas, se recopilen adecuadamente y sean admisibles en los tribunales. A nivel internacional, organizaciones como Europol facilitan la cooperación transfronteriza coordinando esfuerzos entre jurisdicciones. La naturaleza global y transparente de la tecnología de «blockchain» respalda aún más esta colaboración, permitiendo que jurisdicciones más avanzadas detecten y compartan información sobre posibles delitos relacionados con las criptomonedas y el blanqueo de capitales, promoviendo intercambios de inteligencia más rápidos y espontáneos entre países.

7. Conclusiones

En conclusión, navegar por el complejo panorama de las investigaciones financieras sobre criptomonedas requiere que las fuerzas del orden estén equipadas con herramientas sólidas, conocimientos integrales y un espíritu de colaboración. A medida que las monedas digitales continúan evolucionando e integrándose a la economía global, también deben hacerlo las estrategias y metodologías empleadas para combatir las actividades ilícitas. Al adoptar tecnologías avanzadas, fomentar la cooperación internacional y mejorar continuamente los marcos normativos, las fuerzas del orden pueden salvaguardar eficazmente la integridad del sistema financiero.

Los retos que plantean los delitos relacionados con las criptomonedas son significativos y polifacéticos, y abarcan conflictos jurisdiccionales, incoherencias jurídicas, brechas tecnológicas y cuestiones de confianza y soberanía. Para abordar estos retos se necesita un esfuerzo concertado y coordinado tanto a nivel nacional como internacional. Las fuerzas del orden deben priorizar la educación y la formación continuas para mantenerse al día de los últimos avances en tecnología de criptomonedas y tácticas delictivas. Aprovechar herramientas como el análisis de «blockchain» y colaborar con unidades especializadas en ciberseguridad será fundamental para mantenerse un paso por delante de los delincuentes.

En última instancia, la lucha contra los delitos relacionados con las criptomonedas requiere un enfoque proactivo y adaptativo. Las fuerzas del orden deben mantenerse vigilantes e innovadoras, perfeccionando continuamente sus estrategias para hacer frente al cambiante panorama de la delincuencia financiera digital. Al adoptar un enfoque holístico e integrado, podemos garantizar que la promesa de las criptomonedas no se vea empañada por su uso indebido, manteniendo un entorno seguro y justo para todos. Mediante la dedicación, la colaboración y la innovación, las fuerzas del orden pueden contrarrestar eficazmente las amenazas que plantean los delitos relacionados con las criptomonedas, protegiendo el sistema financiero y defendiendo el estado de derecho en la era digital.

Federico Paesano

Investigaciones financieras y análisis para riesgos emergentes de blanqueo de capitales:

Uso delictivo de criptomonedas

Financiado por la Unión Europea

COPOLAD