Las criptomonedas y las investigaciones por lavado de activos

Federico Paesano
Especialista superior en investigación financiera

Hasta ahora ha sido un viaje increíble. La primera vez que oí hablar de Bitcoin fue en 2010 en una conferencia sobre ciberdelincuencia. Aún no sabíamos mucho, salvo que era una nueva forma de dinero – completamente descentralizada, ya que no era emitida ni controlada por ningún gobierno – y que tenía la posibilidad de ayudar a los delincuentes a mover y blanquear sus ganancias a través de las fronteras sin ser detectados.

¿Cómo puede ser descentralizado el dinero? ¿Pueden los delincuentes convertir sus fondos mal habidos en bitcoins y volverlos a fiduciarios? ¿Se acabó el juego para las agencias de aplicación de la ley si la adopción de Bitcoin crece exponencialmente? Estas eran nuestras preguntas en aquel momento.

La respuesta a la última pregunta parecía ser un gran "sí", ya que se había empezado a detectar actividad delictiva en este campo y aún parecía imposible investigar los flujos de criptomonedas en la blockchain. El uso de Bitcoin parecía ser la herramienta de anonimato definitiva.

Atención creciente

Cuando el Basel Institute on Governance decidió sentarse con la Organización Internacional de Policía Criminal (INTERPOL) y la Agencia de la Unión Europea para la Cooperación Policial (Europol) en el año 2014, el tema correspondía a un nicho muy pequeño.

En aquella época existía solamente una criptomoneda (Bitcoin), solo había ocurrido un caso que se podía analizar (Silk Road), y sólo éramos 20 personas reunidas en un pequeño salón de la Universidad de Basilea. A pesar de eso, decidimos fundar conjuntamente un Grupo de Trabajo sobre criptomonedas y lavado de activos. Presentíamos que algo muy grande estaba ocurriendo, y que las agencias de aplicación de la ley debían estar preparadas para enfrentar el desafío.

Pero ¡qué cambio en tan solo unos años! Hoy en día, miles de personas solicitan asistir cada año a nuestra Conferencia Mundial sobre Finanzas Delictivas y Criptomonedas. Existen cientos de nuevas criptomonedas y otras formas innovadoras de activos virtuales, como los tokens no fungibles y las divisas digitales de los bancos centrales, y cada vez son más los casos de lavado de activos que obligan a los investigadores a adentrarse en la "criptoesfera".

Los reguladores mundiales también se están tomando el asunto más en serio. El Grupo de Acción Financiera (GAFI), el organismo de control mundial del lavado de activos, ha publicado normas y pautas actualizadas sobre activos virtuales y proveedores de servicios de activos virtuales (VASP, por sus siglas en inglés), y está monitoreando de cerca los avances de los Gobiernos en materia de su cumplimiento.

Y en junio de 2023, la Unión Europea adoptó el marco regulador más amplio para los activos digitales hasta la fecha: el Reglamento sobre Mercados de Criptoactivos (MiCA).

¿En qué clases de delitos se utilizan las criptomonedas?

Las criptomonedas tienen muchos beneficios y usos legítimos, como el potencial de ofrecerles un sistema de pagos internacionales de bajo precio, rápido y accesible a millones de personas de todo el mundo que no tienen acceso a servicios bancarios. Pero, al igual que cualquier reserva de valor, se podrían usar de forma indebida.

En algunos casos, los delincuentes utilizan las criptomonedas para lavar las ganancias "normales" derivadas de un delito o de la corrupción. Un ejemplo sencillo sería el de un funcionario corrupto que recibe sobornos y trata de ocultar el origen de estos fondos al transferirlos desde y hacia varias criptomonedas y monedas fiduciarias, como los dólares.

Sin embargo, en la mayoría de los casos hablamos de delitos que generan ingresos en criptomonedas. Como se describe en el informe Evaluación de

las Amenazas del Crimen Organizado en Internet (IOCTA, por sus siglas en inglés) publicado por la Europol, las criptomonedas se utilizan para facilitar los pagos de diferentes actividades ilícitas.

Entre ellas se encuentran el tráfico de drogas y otros bienes ilegales en la *dark web*, programas de *ransomware* (o secuestro de datos) como Rhysidia o Abyss, pago por secuestros y rescates, y delitos cibernéticos.

Seguir el rastro del dinero virtual: fácil en algunos casos, más problemático en otros

En teoría, la tecnología de *blockchain* (cadena de bloques) en la que se basan las criptomonedas hace más fácil que los investigadores financieros sigan el rastro del dinero. ¿Por qué?

Porque todas las operaciones se capturan permanentemente en un registro contable compartido (la cadena de bloques) que no se puede alterar ni modificar. En teoría, el rastro del dinero nunca desaparecería, y se podría convertir en evidencia incluso años después.

El reciente procesamiento de un individuo que robó más de 50.000 bitcoins de la extinta bolsa de criptomonedas MtGox en 2012 ilustra claramente este proceso. La inmutabilidad de la *blockchain* permitió a los investigadores seguir el rastro del dinero, identificar al culpable y recuperar activos por un valor récord de USD 3.36 mil millones casi diez años después de los hechos.

Esto no sería posible con transacciones en efectivo, por ejemplo. Es imposible devolver el tiempo y saber quién le dio qué a quién.

Las operaciones de Bitcoin incluyen la fecha, hora y monto, así como las direcciones del remitente y del beneficiario (en forma de seudónimos compuestos por largas secuencias de caracteres alfanuméricos). En comparación, las criptomonedas menos conocidas y más enfocadas en la privacidad, como Monero, ocultan esta información.

En cualquier caso, el problema yace en la *atribución:* es decir, en cómo vincular las operaciones y las direcciones a personas reales en el mundo real. En otras palabras, se trata de identificar las operaciones posiblemente delictivas y a los delincuentes que las llevan a cabo.

Romper las barreras del anonimato

Por suerte para los investigadores, existen técnicas para penetrar en el evidente anonimato de las criptomonedas y vincular las operaciones y las direcciones a presuntos delincuentes y lavadores de activos.

Por ejemplo, se puede usar la heurística para crear *clusters,* es decir, grupos de direcciones que probablemente sean controladas por la misma entidad. Después, se aplican técnicas especiales para desanonimizar estos *clusters.*

Es en este punto que las firmas de análisis de la cadena de bloques pueden ayudar. A cambio de una tarifa, estas firmas pueden analizar las direcciones y las operaciones para obtener información vital, como datos de geolocalización o cuál fue la plataforma de intercambio que se utilizó para comprar las criptomonedas.

Posteriormente, los investigadores pueden solicitar más información a esta plataforma, de la misma forma en que se solicitaría a un banco o cualquier otro proveedor de pagos. A medida que las normas del GAFI sobre VASP mencionadas anteriormente se implementan por medio de las legislaciones nacionales, esperamos y confiamos que estas plataformas pongan a disposición de las autoridades competentes datos más confiables sobre sus clientes.

El costo de consultar a una firma de análisis de la cadena de bloques podría representar un obstáculo en los países con recursos limitados para la aplicación de la ley.

Sin embargo, la mayoría de las investigaciones relacionadas con las criptomonedas de hecho comienzan con los sospechosos, y no con una transacción misteriosa o una dirección anónima. Los investigadores simplemente tratan de determinar qué direcciones de criptomonedas controla un sospechoso. A menudo, esta información se puede revelar por medio de análisis forenses de los dispositivos del sospechoso, sin necesidad de consultar a una firma de análisis de cadena de bloques.

Por qué los peritos son de ayuda en el procesamiento de los casos

La naturaleza relativamente nueva y en constante evolución de los activos virtuales implica que no existe un conocimiento general de las tecnologías de las cadenas de bloques como las criptomonedas.

Esto es válido en el caso de los funcionarios de los organismos judiciales y de aplicación de la ley, quienes podrían verse en la necesidad de interpretar evidencias derivadas del análisis de la cadena de bloques o billeteras digitales para condenar a un sospechoso.

En este caso, es útil llamar a un perito al tribunal para que ayude a aclarar y verificar este tipo de evidencias. Naturalmente, una explicación clara de los pasos del proceso de investigación también sería útil para demostrarle al tribunal que la evidencia así recolectada se puede utilizar de la misma manera que cualquier otra evidencia de un delito financiero.

Recuperar los activos robados representados en criptomonedas

Los activos que están representados en criptomonedas se pueden abordar de la misma manera que los activos representados en cuentas bancarias o bienes inmuebles. Por ejemplo, un juez puede ordenar el embargo preventivo de los activos en una cuenta de criptomonedas mientras se llega a un fallo en el caso.

Las operaciones en criptomonedas se pueden realizar en cuestión de minutos; por este motivo, es necesario que se agilice la cooperación internacional en materia del embargo preventivo de activos. Incluso en el caso de las transferencias bancarias ordinarias, durante el tiempo que tarda expedir la orden de embargo preventivo, el dinero ya podría haber circulado varias veces por muchos lugares del mundo.

Cuando se trata de decomisar y recuperar activos representados en criptomonedas, las autoridades (que aún utilizan las monedas fiduciarias, pero, ¿quién sabe si ese seguirá siendo el caso en el futuro?) tienen varias opciones.

- Una de ellas es utilizar una plataforma de intercambio para convertir las criptomonedas a la moneda fiduciaria relevante.

- Otra opción es realizar una subasta. El Departamento de Justicia de los EE. UU. recuperó casi USD 50 millones luego de subastar una gran cantidad de bitcoins ilícitos tras la clausura del mercado en línea Silk Road en el 2013.

La volatilidad en el mercado de las criptomonedas es un dolor de cabeza para las personas a cargo de la recuperación de los activos. Si se hubiera realizado hoy, la subasta de 144 336 bitcoins de Silk Road habría generado alrededor de USD 4.2 mil millones.

¿Qué pueden hacer los organismos de aplicación de la ley?

En la 6ª Conferencia Global sobre Criptomonedas y Finanzas Criminales de 2022, coorganizada por el Basel Institute y EUROPOL, y a la que asistieron más de 2.000 participantes presenciales y a distancia, se formularon cinco recomendaciones producto de los debates.

1. **Romper los silos entre lo "tradicional" y lo "cripto"** – no tratar lo cripto como un área separada, sino operar a través de los dominios físico y virtual (como hacen los delincuentes).

2. **Regular ampliamente y hacer pleno uso de las leyes existentes** – para garantizar que los criptoactivos sean tratados como cualquier otro activo a efectos de supervisión, aplicación y recuperación de activos en materia de ALA/CFT.

3. **Aprovechar la blockchain para desarticular el crimen organizado** – ya que la blockchain ofrece numerosas oportunidades para investigar y desarticular esquemas delictivos y de blanqueo de capitales, recopilar inteligencia y congelar y confiscar activos ilícitos.

4. **Aumentar la alfabetización en criptomonedas mediante el desarrollo de capacidades y una comunicación clara** – eliminando la jerga y los acrónimos y extendiendo una formación básica en criptomonedas a grupos más amplios de personal.

5. **Aumentar la cooperación público-privada** – ya que las fuerzas de seguridad pueden ganar mucho de las habilidades técnicas de las empresas de rastreo de activos y análisis de blockchain, así como cooperar con los proveedores de servicios de criptoactivos para acelerar las órdenes de congelamiento de cuentas y el intercambio de información.

Publicado originalmente en inglés el 15 de marzo de 2019 y actualizado el 11 de agosto de 2023. Todas nuestras guías rápidas están disponibles en learn.baselgovernance.org

ISSN 2673–5229

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

+41 61 205 55 11
info@baselgovernance.org
baselgovernance.org

@BaselInstitute
Basel Institute

The Basel Institute on Governance is an Associated Institute of the University of Basel