- 2023 -

Guía práctica para la identificación, trazabilidad e incautación de criptoactivos

Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal

—

MPF | Ministerio Público Fiscal de la Nación

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Guía práctica para la identificación, trazabilidad e incautación de criptoactivos

Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal

---

Documento elaborado por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

Fiscal: Horacio J. Azzolin

Con la colaboración de:

Procuraduría de Criminalidad Económica y Lavado de Activos (PROCELAC)

Secretaría de Análisis Integral del Terrorismo Internacional (SAIT)

Secretaría de Coordinación Institucional (SCI)

Dirección General de Recuperación de Activos y Decomiso de Bienes (DGRADB)

Procuraduría de Narcocriminalidad (PROCUNAR)

Unidad Fiscal Especializada en Secuestros Extorsivos (UFESE)

Procuraduría de Trata y Explotación de Personas (PROTEX)

Diseño: Dirección de Comunicación Institucional

Publicación: abril 2023

- 2023 -

Guía práctica para la identificación, trazabilidad e incautación de criptoactivos

Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal

—

MPF | Ministerio Público Fiscal de la Nación

Índice

1. INTRODUCCIÓN

El 31 de octubre de 2008, bajo el nombre –o seudónimo– de "Satoshi Nakamoto", se publicó un documento titulado *"Bitcoin: A Peer–to–Peer Electronic Cash System"*[1], con el que se presentó en sociedad el proyecto para la creación del primer activo digital que se describió como *"Una versión puramente electrónica de efectivo [que] permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera"*.

Desde esos primeros días hasta la actualidad, Bitcoin ha crecido enormemente, tanto en valor como en su alcance, y ha dado lugar al surgimiento de nuevas propuestas basadas en técnicas criptográficas y en su innovador modelo de base de datos: la cadena de bloques o "blockchain". Estos desarrollos conforman un ecosistema vasto, complejo y en permanente expansión, en el que coexisten miles de proyectos con particularidades de naturaleza variada, cuyos precios y niveles de aceptación por parte de la comunidad fluctúan significativamente, habiendo llegado a alcanzar el valor total de mercado un máximo cercano a los tres billones de dólares en los últimos tiempos[2].

Como ocurre con cualquier tecnología novedosa, nos encontramos con usuarios atraídos por sus bondades, interesados en explorar sus posibles beneficios sociales y económicos, pero también con individuos que desnaturalizan su propósito y evalúan alternativas para explotar la tecnología en el marco de actividades ilícitas. Los beneficios e innovaciones que este tipo de activos presentan, su desregulación, su masiva proliferación o el uso de diversas tecnologías, aparejaron nuevos riesgos, al crear nuevas oportunidades para que, por ejemplo, los lavadores de dinero, los financiadores del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas. La capacidad de realizar operaciones transfronterizas rápidamente y a través de internet no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, pero también disfrazar el origen o destino de los recursos y dificultar que los sujetos obligados identifiquen las actividades sospechosas de manera oportuna. Estos factores añaden obstáculos a la detección e investigación de la actividad criminal por las autoridades nacionales[3].

Es ahí donde la investigación criminal ligada a los criptoactivos cobra un rol preponderante. Con el paso del tiempo se observa un aumento en la adopción de esta tecnología por parte de diferentes organizaciones criminales, no solo en casos expresamente vinculados a la ciberdelincuencia –como, por ejemplo, ataques informáticos del tipo "ransomware"[4]–, sino también en otro tipo de actividades

1. https://bitcoin.org/bitcoin.pdf

2. De acuerdo a CoinMarketCap (https://coinmarketcap.com) –una plataforma creada para realizar un seguimiento de la capitalización de diferentes criptoactivos, la cantidad de operaciones que las utilizan y el precio actual convertido a monedas fiduciarias– el 21 de noviembre de 2021 el valor de mercado de los criptoactivos circulantes alcanzó un máximo de U$D 2.973.212.260.893.

3. Informe del GAFI (2020) "Activos Virtuales señales de alerta de LD / FT", https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traducciones/3873-informe-del-gafi-activos-virtuales-senales-de-alerta-de-ld-ft

4. Ransomware o "secuestro de datos", es un tipo de maniobra informática que involucra el uso de programas maliciosos que restringen mediante cifrado el acceso a determinadas partes o archivos del equipo infectado, para luego solicitar un rescate a cambio de las claves de acceso que permitan quitar dicha

criminales como lavado de activos, narcotráfico y financiamiento del terrorismo[5]. Se advierte además que, a medida que su uso se extiende en las sociedades, es cada vez más común encontrarse con delitos de menor complejidad atravesados por esta clase de activos.

Teniendo en cuenta que en la Argentina el grado de inserción de los criptoactivos es particularmente alto –ubicándose en el puesto 13° a nivel global, de acuerdo al informe "Índice Global de Adopción de Criptoactivos 2022"[6] elaborado la empresa Chainalysis–, se advierte la necesidad de redoblar los esfuerzos e incrementar la capacidad del Ministerio Público Fiscal para abordar aquellos casos atravesados por este tipo de desarrollos y sus complejos aspectos técnicos.

Este documento tiene por objeto brindar una serie de definiciones básicas que caracterizan el ecosistema de los criptoactivos y la tecnología de cadena de bloques sobre la que se sustentan, para luego realizar un abordaje integral sobre diferentes aspectos investigativos vinculados con la trazabilidad e identificación de transacciones, posibles evidencias forenses e incautación de este tipo de activos virtuales.

restricción.

5. En este sentido, programa El PACcTO (2022), "Guía de investigación en el lavado de activos mediante criptodivisas", https://www.elpaccto.eu/wp-content/uploads/2022/07/Guia-Lavado-Activos-Criptodivisas.pdf. Véase también Europol (2022), "Cryptocurrencies: Tracing the Evolution of Criminal Finances, Europol Spotlight Report series", https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf; GAFILAT (2021) "Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales", https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/guias-17/4225-gui-a-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigacio-n-identificacio-n-incautacio-n-y-decomiso-de-av/file.

6. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

2. NOCIONES BÁSICAS SOBRE CRIPTOACTIVOS, CLASIFICACIONES Y DENOMINACIONES.

Para dar los primeros pasos en la temática, resulta importante introducir ciertos aspectos ligados a la terminología y definiciones propias del ecosistema.

En este sentido, existen algunos conceptos con los que se suele hacer mención a esta clase de activos, cuyos alcances, en ocasiones, resultan algo difusos o disímiles, dependiendo de quién lo utilice. Se trata de una tecnología novedosa, por lo que ciertos términos y definiciones se encuentran en vías de ser estandarizados y aceptados universalmente. No nos adentraremos en las discusiones vigentes en torno a ello, sin embargo, conceptualizaremos a continuación a qué nos referiremos en el presente documento cuando utilicemos aquellos términos.

2.1. Activos Virtuales (AV)

Se trata de un término adoptado por diferentes organismos internacionales para referirse a los activos de esta naturaleza. El Grupo de Acción Financiera Internacional (GAFI)[7] define a los activos virtuales como *"una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias*[8]*, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del organismo"*, conforme se desprende de la "Guía para un enfoque basado en el riesgo de activos virtuales y proveedores de servicios de activos virtuales"[9].

En términos similares, la Unidad de Información Financiera (UIF), en su resolución 300/2014 (4/07/2014)[10] definió a las "Monedas Virtuales" como la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En ese sentido, la UIF diferenció a las monedas virtuales del "dinero electrónico", entendido este último como un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción.

---

7. El Grupo de Acción Financiera Internacional (en inglés, Financial Action Task Force), es una institución intergubernamental cuyo propósito es desarrollar políticas que ayuden a combatir el blanqueo de capitales y la financiación del terrorismo.

8. Se consideran monedas fiduciarias a todas aquellas divisas nacionales que no se encuentran vinculadas al precio de una materia prima, como el oro o la plata. El valor de una moneda fiduciaria se basa en gran medida en la confianza pública en el expedidor de la moneda, que es habitualmente el banco central o el gobierno de un país. Así, por ejemplo, podemos mencionar la libra esterlina, el euro y el dólar estadounidense.

9. GAFI (2021), "Updated guidance for a risk-based approach. Virtual Assets and Virtual Asset Service Providers", https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

10. http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm

Entonces existe cierto consenso al caracterizar a Bitcoin y a los demás desarrollos que comparten sus aspectos elementales como activos virtuales, distinguiéndolos mediante esta clasificación de los activos digitales, es decir, las representaciones digitales de monedas fiduciarias u otros activos.

2.2. Criptoactivos

En términos generales, podría decirse que "criptoactivo" es la denominación que recibe cierto tipo de activos virtuales que se diferencian de los demás por cómo son implementados, es decir, por funcionar sobre una plataforma que se vale del uso de técnicas criptográficas y de una base de datos constituida sobre un sistema de cadena de bloques.

Nos encontramos ya ante un concepto con el que podemos caracterizar exclusivamente a los activos que nos ocupan en el presente documento. Sin embargo, cabe mencionar que no se trata de un término técnico-jurídico, sino sólo de una denominación, aceptada dentro del ecosistema, que nos va a permitir distinguir a esta clase de activos de otros tipos de activos virtuales.

Como se mencionó anteriormente, existe una amplia variedad de criptoactivos: más de 23.000, de acuerdo a la plataforma CoinMarketCap[11], en un ecosistema en permanente expansión y fluctuación en donde cada proyecto goza de algunas particularidades. En diversas ocasiones se han intentado clasificaciones que fueran capaces de abarcar a todos los subtipos de activos, sin embargo, el dinamismo propio del ecosistema y el volumen de proyectos dificultan dicha labor.

De todos modos, delinearemos a continuación algunas categorías y conceptos sobre los que existe cierto consenso. Por un lado, para graficar –aunque más no sea parcialmente– el universo de plataformas que coexisten hoy en día, pero fundamentalmente, para explicitar el alcance que se le dará a ciertos términos propios de la temática a lo largo del presente documento.

2.2.1) Clasificación según su implementación

2.2.1.1) Criptomonedas

Existe un debate sobre el uso de esta denominación, en tanto los activos analizados, por sus características, no podrían encuadrar dentro de la categoría "moneda". Nos limitaremos a señalar que, al igual que en el caso anterior, no se trata de un concepto técnico-jurídico, sino de una designación adoptada en el ecosistema para referirse a cierta clase de criptoactivos.

A los efectos del presente trabajo, optamos por utilizar el término "criptomoneda" para referirnos

11. https://coinmarketcap.com (consultado el 12/04/2023).

exclusivamente a los activos nativos de plataformas basadas en técnicas criptográficas y que se valen de una base de datos constituida bajo el sistema de cadena de bloques. Ocurre que, como veremos luego, algunos desarrollos les permiten a sus usuarios desplegar sobre la cadena de bloques líneas de código informático y ejecutable, lo que da lugar a la posibilidad de generar nuevas plataformas de criptoactivos que funcionen sobre las anteriores.

2.2.1.2) *Tokens*

Nuevamente, nos encontramos con un término que acepta una amplia gama de interpretaciones. A lo largo del presente documento, nos referiremos a los "tokens" por oposición a las criptomonedas. Consideraremos a los "tokens" activos no nativos que funcionan sobre plataformas como las descriptas, desplegados e implementados por medio de programas informáticos conocidos como "contratos inteligentes".

Los "tokens" son susceptibles de presentar funcionalidades similares a las de las criptomonedas, aunque su creación enfrenta menos obstáculos, ya que no requieren para su funcionamiento del despliegue de una red dedicada de usuarios que adopten su sistema y conformen la infraestructura necesaria para el funcionamiento de un sistema de cadena de bloques que goce de cierta estabilidad y confiabilidad. De ahí que gran parte de los criptoactivos con los que podemos encontrarnos funcionen del modo descripto.

2.2.2) Denominaciones según las particularidades del activo y su función

2.2.2.1) *Depósitos de valor*

Si tenemos en cuenta la capitalización del mercado, Bitcoin es la criptomoneda que acapara el mayor volumen de transacciones. Como ya se indicó, habría sido creada con el supuesto objetivo de constituirse como un medio de pago alternativo a las monedas y divisas que conocemos y utilizamos en nuestra vida diaria, con la particularidad que funcionaría en forma electrónica y sin una autoridad central que la regule.

En la actualidad, suele utilizarse para adquirir bienes y servicios, aunque también ha sido adoptada en gran medida como un medio para el resguardo de ahorros, como así también, para obtener un rédito mediante la compraventa de dicho activo en los mercados especulativos, aprovechando las fluctuaciones de su cotización.

Comúnmente se distingue a los activos utilizados como reserva de valor de aquéllos que se utilizan principalmente como medio de pago. Entendemos que se trata de una distinción con un alto margen de subjetividad, en tanto en todos los casos en los que tratemos con criptoactivos que se ofrezcan a un precio, encontraremos usuarios que prioricen su uso para uno u otro cometido.

Otras clasificaciones optan por separar esta categoría de activos de aquéllos que son generados y distribuidos, por ejemplo, para otorgarle a sus tenedores derechos a gozar de determinados bienes o servicios, o a percibir ganancias futuras, a la vez que plantean subclasificaciones en las que enmarcan estos y otros supuestos de uso.

Dentro del ecosistema de los criptoactivos constantemente se generan nuevos proyectos innovadores que se apartan total o parcialmente de estas categorías, lo que obliga a una revisión, rectificación y/o ampliación constante, desnaturalizando así el valor de una clasificación basada en estos aspectos.

En cualquier caso, en la medida que estos activos posean un valor en el mercado, podrían ser considerados depósitos de valor.

2.2.2.2) *Altcoins*

En general, cualquier criptoactivo basado en la tecnología "*blockchain"* que no sea Bitcoin se denomina "altcoin", término que surge justamente de la abreviatura de "alternativa a Bitcoin".

Su popularidad se encuentra ligada a diferentes factores, sin embargo, la capitalización del mercado posiciona a ciertas "altcoins" como las preferidas por los usuarios al momento de realizar operaciones con criptoactivos.

A modo de ejemplo, podemos mencionar a Ether: la criptomoneda nativa del sistema denominado Ethereum, el cual constituye, además del sostén tecnológico del referido activo, una plataforma sobre la cual se despliegan otro tipo de desarrollos tecnológicos, entre los que se destacan los contratos electrónicos.

Esto último, sumado a su valor y su gran adopción por parte de la comunidad, permiten caracterizarla como uno de los principales criptoactivos del mercado, posicionándose como la segunda alternativa preferida, inmediatamente después de Bitcoin. Sin perjuicio de ello, Ether puede ser considerada una "altcoin".

2.2.2.3) *Criptoactivos estables*

Como se señaló, tanto Bitcoin, como las "altcoins" son susceptibles de poseer un valor en el mercado. Como ocurre con otros activos, el valor de los criptoactivos se ve atravesado por las reglas de la oferta, la demanda y otras variables económico-financieras, y ocurre que suele presentar un alto grado de volatilidad.

La volatilidad puede significar un problema para quienes utilizan esta clase de activos para realizar y recibir pagos o como un medio para resguardar sus ahorros. Aquéllos que negocian y especulan con

criptoactivos, si bien buscan predecir y aprovechar estas fluctuaciones, encuentran también provechosa la posibilidad de incluir, entre los activos con los que operan, uno cuyo valor sea relativamente estable para poder ingresar y retirarse de sus posiciones sin salirse del ecosistema.

Tal es así que, al día de hoy, los criptoactivos estables –como Tether, DAI y USDCoin, entre otros– juegan un rol fundamental dentro del entorno, e incluso cumplen un rol como punto de entrada para un gran número de personas que desean ingresar al mundo de los criptoactivos, ya que suelen considerarlos una alternativa más segura y menos propicia a las fluctuaciones que suelen caracterizar a otros activos.

Múltiples desarrollos intentaron afrontar la demanda de un activo estable mediante diferentes abordajes, principalmente, erigiéndose como "tokens", es decir, como contratos inteligentes, sobre otras plataformas. Nos encontramos, por ejemplo, con criptoactivos colateralizados, es decir, que poseen un respaldo en otro tipo de activos, y otros que no presentan esa característica.

En lo que respecta a los primeros, el respaldo puede ser de diferente naturaleza, desde dinero fiduciario hasta criptoactivos de orden diverso. Los restantes se rigen exclusivamente por protocolos que regulan, por ejemplo, la emisión y la absorción de activos, incidiendo de ese modo sobre la oferta y demanda de modo tal que el valor se mantenga estable.

Por otra parte, ciertos aspectos vinculados al funcionamiento del sistema y los recursos para regular su valor pueden ser centralizados y, en consecuencia, ser controlados por quien o quienes se encuentren detrás del proyecto. También es posible desarrollar este tipo de proyectos de manera tal que logren niveles elevados de descentralización, mediante protocolos a través de los cuales los distintos procesos necesarios para su implementación pueden ser automatizados.

Los activos que cuentan con respaldo en una moneda fiduciaria suelen ser parcialmente centralizados, en tanto es preciso que una autoridad administre el respaldo monetario y dosifique la emisión y la absorción de unidades del criptoactivo para mantener la paridad. Otros proyectos, especialmente aquéllos no colateralizados o apalancados con criptoactivos, pueden prescindir de ello, lo que permite que sean implementados con un alto grado de descentralización.

2.2.2.4) *Token no fungible (NFT)*

Un token no fungible o NFT *("Non fungible token")* es un activo criptográfico que tiene la capacidad de ser único e irrepetible. Los tokens de este tipo no pueden ser divididos, pero si utilizados para representar objetos del mundo real o digital junto a sus características propias, así como la propiedad del mismo.

El funcionamiento de los NFT o "tokens" no fungibles depende de contratos inteligentes ejecutados

en una cadena de bloques determinada como, por ejemplo, la plataforma Ethereum.

2.2.2.5) *Oferta Inicial de criptoactivos (ICO)*

Las ofertas iniciales de moneda o "Initial Coin Offering" –ICO– tienen como finalidad conseguir financiación de una iniciativa o proyecto mediante la emisión de una criptomoneda o "token" desarrollado sobre la tecnología de cadena de bloques.

Una ICO es el proceso por el cual un criptoactivo se distribuye mediante la venta anticipada de unidades en una fase temprana de desarrollo del proyecto. Dicho activo podrá usarse en el proyecto en sí, lográndose cumplir con su principal objetivo de financiación.

3. LA CADENA DE BLOQUES

La principal característica de Bitcoin y otros criptoactivos similares es que no se encuentran sujetos al control y respaldo de una institución central que cumpla la labor de emitirlos, sino que funcionan de manera descentralizada, a través de una red sin intermediarios "peer to peer" (P2P) conformada por nodos que -en la mayoría de los casos- cualquier persona puede montar, lo que, sumado al uso de funciones "hash"[12] y técnicas de criptografía asimétrica, les otorga un elevado nivel de seguridad.

3.1. Blockchain

La cadena de bloques o "blockchain" es el desarrollo tecnológico fundacional de los criptoactivos. Es una base de datos que posee similitudes con aquéllas basadas en la tecnología de registro distribuido (DLT o "Distributed Ledger Technology"), pero posee ciertas características para garantizar su integridad que la distinguen de cualquier otra. Concretamente, los datos no se incorporan sucesivamente, uno a uno, sino que se agrupan en un "bloque", el cual se agrega a la "cadena". Cada bloque nuevo incorpora, entre sus datos, el resultado de la aplicación de una función "hash" sobre el bloque anterior, por lo que, si se modifica un dato en un bloque anterior, el valor "hash" de ese bloque se alteraría y, por ende, no coincidirá con aquel registrado en el bloque siguiente.

Cabe destacar que esta tecnología, tiene sus orígenes en 1991, cuando Stuart Haber y W. Scott Stornetta describieron el primer trabajo sobre un sistema de jerarquía digital asegurado criptográficamente llamado "cadena de bloques". El estudio, titulado "Como hacer una marca de tiempo en un documento digital"[13], tuvo como finalidad crear mecanismos para generar un sello de tiempo digital y ordenar los archivos registrados de forma única y segura para que no pudieran ser modificados o manipulados.

La cadena de bloques se encuentra almacenada y replicada en miles de nodos interconectados alrededor del mundo, montados por los propios usuarios de la red, los cuales verifican la validez de cada uno de los bloques que se adicionan. Las operaciones, cabe mencionar, también son procesadas por los propios usuarios en gran parte de los desarrollos de esta naturaleza.

Si bien la cadena de bloques generalmente se asocia con el Bitcoin y otras criptomonedas, estas implementaciones son solo una muestra de la potencialidad de la tecnología, dado que actualmente su utilización es demandada en otras aplicaciones comerciales y se proyecta un crecimiento exponencial en varios mercados, como el de las instituciones financieras o el de Internet de las Cosas (IoT).

---

12. La función Hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). Estas funciones tienen varios cometidos, entre ellos está demostrar que no se ha modificado un archivo en una transmisión.

13. https://link.springer.com/content/pdf/10.1007/BF00196791.pdf

3.2. Estructura de un bloque

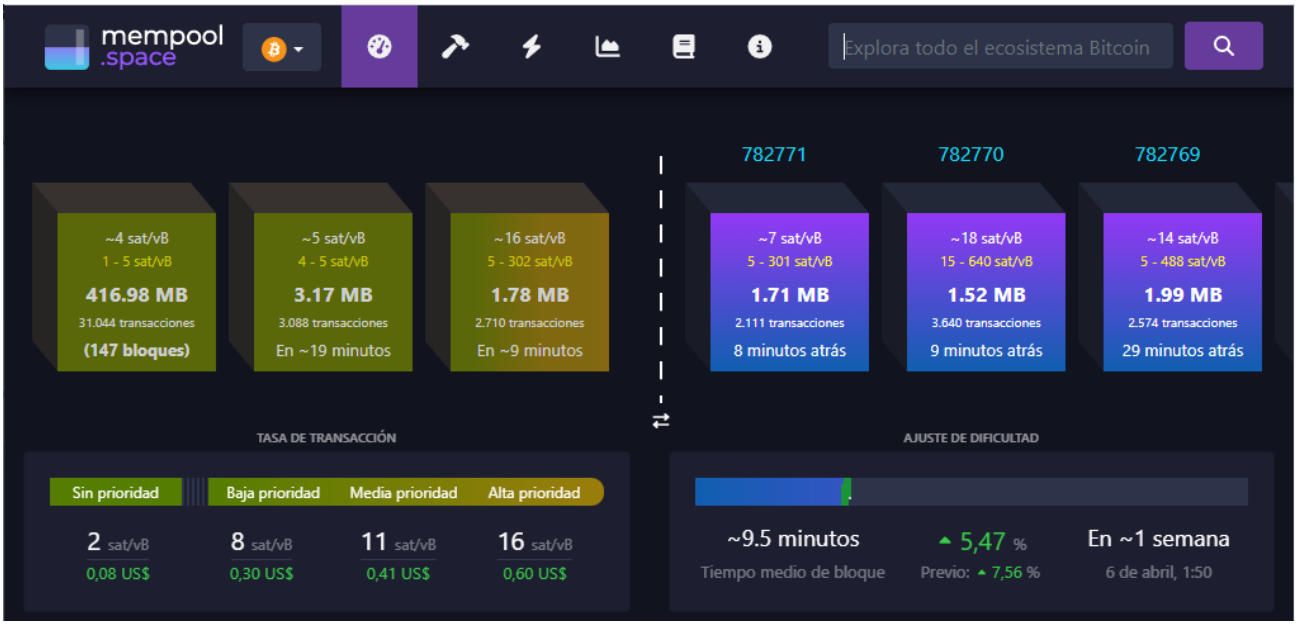
Como se mencionó anteriormente, la "blockchain" es una cadena de bloques en la que cada bloque se compone de una serie de transacciones agrupadas. Cada nuevo bloque se vincula criptográficamente a los bloques que lo precedieron, al mismo tiempo que almacena información referente a ese bloque en particular.

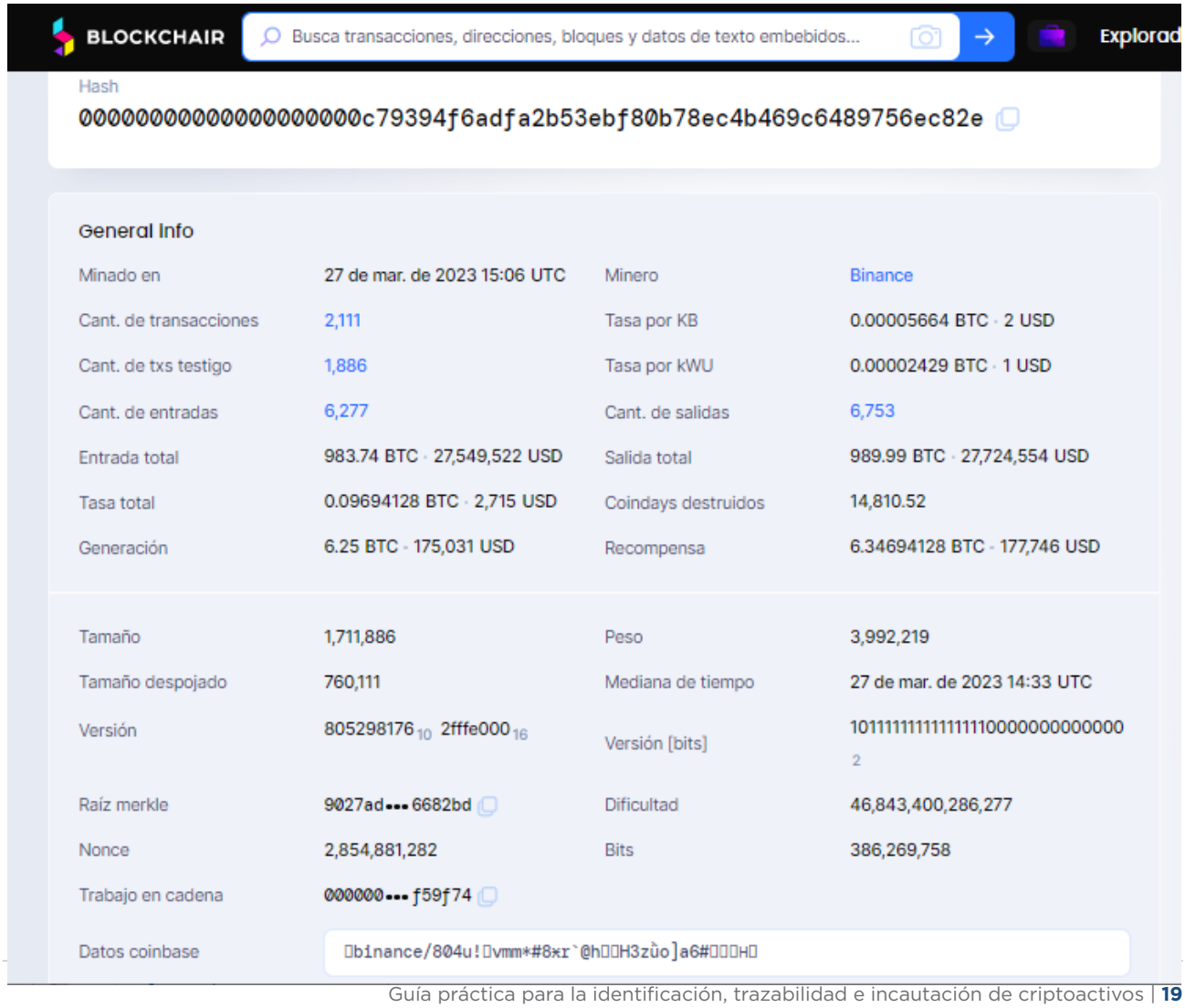
Para comprender la estructura de un bloque, nos centraremos en Bitcoin. En su cadena de bloques, que lleva un registro contable público de transacciones entre direcciones, cada bloque "minado" contiene una cantidad significativa de información, entre la que se encuentra:

- Valor "hash" del bloque
- Orden del bloque en la cadena de bloques
- Volumen total de las transacciones
- Comisiones por las transacciones
- Tamaño real del bloque
- Tamaño Virtual del bloque
- Versión de Software utilizado para crear el bloque
- Marca de tiempo de la hora en que se incluyó el bloque en la cadena de bloques
- Bits utilizados para indicar el objetivo/dificultad
- "Nonce" o número utilizado para crear aleatoriedad y que los mineros calculen el "hash" de bloque adecuado
- Cantidad de transacciones que conforman el bloque
- "Hash" del bloque anterior en la cadena de bloques
- "Hash" de nivel superior vinculado a la raíz de Merkle[14]

14. Un árbol de Merkle o árbol "hash" binario es una estructura de datos usada en la "blockchain" que sirve para resumir y verificar la integridad de una base de datos, constituyendo una parte fundamental de la cadena de bloques. Este sistema recibe su nombre de Ralph Merkle, quien desarrolló el mecanismo en 1979 para agilizar la comprobación de grandes bloques de datos. Se caracteriza por ser una estructura ramificada, como un árbol invertido, en la que se parte desde los nodos base (hojas) y se escala progresivamente a través de nodos padre (ramas) hasta llegar al nodo raíz o Merkle root. Este último es el identificador principal que permitirá verificar el conjunto de datos como un todo.

- Lista de transacciones incluidas en el bloque





Los ejemplos ilustrados corresponden a capturas de pantalla de la cadena de bloques y un bloque en particular de la red Bitcoin graficados por diferentes plataformas de análisis[15].

3.3. Disponibilidad e integridad en la cadena de bloques

Al ser una tecnología distribuida, donde cada nodo de la red almacena una copia exacta de la cadena, se garantiza la disponibilidad de la información en todo momento. En caso de que un atacante quisiera provocar una denegación de servicio, debería anular todos los nodos de la red, ya que basta con que al menos uno esté operativo para que la información esté disponible.

Del mismo modo, debido a que los bloques se encuentran enlazados criptográficamente, a medida que se vinculan nuevos bloques, resulta más difícil matemáticamente, o quizás imposible, modificar una transacción que se encuentra incrustada en la cadena de bloques previamente, la que permanecerá íntegra, permaneciendo de forma inalterable y perpetua.

Sin embargo, desde el punto de vista teórico, un atacante que controla un porcentaje significativo de los nodos de una red podría lanzar lo que se conoce como el "ataque del 51%". Si este supuesto atacante controlara más de la mitad de los nodos de una red, sería hipotéticamente posible recalcular varios bloques anteriores y crear una nueva bifurcación en la cadena.

3.4. Bifurcaciones

Las bifurcaciones o "forks" en una cadena de bloques suelen considerarse complejas, pero a fin de ilustrar este concepto de una manera sencilla podríamos compararlo como una bifurcación en un camino donde existen dos vías posibles para continuar. Si registramos y analizamos el recorrido de aquéllos que lo transitan nos encontraríamos, en definitiva, con dos recorridos distintos, más allá de que los registros del tramo previo a la bifurcación coincidan en ambos casos.

Algo similar ocurre cuando, dentro de una plataforma de esta naturaleza, se plantean modificaciones en el sistema o se deben tomar otro tipo de decisiones que conllevan una respuesta heterogénea entre los usuarios. Estas respuestas alternativas pueden dar lugar a bifurcaciones, es decir, a cadenas de bloques paralelas, con una raíz de registros coincidentes pero que difieran a partir de aquel punto.

Según su naturaleza existen diferentes tipos de "forks", que impactan de forma diferente en la cadena de bloques y la manera en que se continuará desarrollando la misma.

15. El ejemplo propuesto fue tomado de https://mempool.space/es/ y https://blockchair.com/es/.

3.4.1) Bifurcaciones huérfanas

Este tipo de bifurcaciones puede darse en el caso hipotético denominado "ataque del 51%", aunque también pueden ocurrir -con mayor frecuencia de lo que podría creerse- por problemas de sincronización de minería.

Por ejemplo, cuando un más de un minero en forma simultánea consigue proyectar un bloque válido y lo comunica a los nodos de la red, nos encontraremos ante múltiples versiones de un bloque identificado con un mismo número de orden, es decir, una bifurcación en la red. Sin embargo, es extremadamente improbable que dos mineros logren conformar simultáneamente un bloque válido que suceda a los anteriores, por lo que la rama de la bifurcación que se extienda primero mediante la adición de un nuevo bloque tenderá a subsistir, mientras que la otra bifurcación queda huérfana. Ello ocurre debido a que los nodos, al comunicarse con otros y constatar que existe una cadena de bloques más extensa que la propia, optarán por descartar la que poseen y hacerse de una copia de esta última.

Cuanto más rápido se configuran los bloques para ser extraídos, más probable es que se encuentren bloques prácticamente al mismo tiempo. Por ejemplo, en la red Bitcoin es de 10 minutos mientras que en Ethereum es de 15 segundos.

3.4.2) Bifurcaciones duras

En el caso de las bifurcaciones duras o "hard forks" los mineros aceptan los cambios recomendados en el software y los protocolos subyacentes que no son compatibles con la cadena de bloques histórica.

Quizás la bifurcación dura más conocida sea Bitcoin Cash, que aumentó el límite máximo de tamaño de bloque de 1 MB a 8 MB, lo que permite alrededor de cuatro veces la cantidad de transacciones por día, un aumento de aproximadamente 250000 a 1 millón. Otro ejemplo es la bifurcación dura de Ethereum a Ethereum Classic, en este caso resulta oportuno señalar que la elección del nombre puede ser un poco engañosa debido a que el actual Ethereum es en realidad la bifurcación y Ethereum Classic es la cadena de bloques original.

Nótese que, en ambos casos, la bifurcación no solo originó un cambio en la cadena de bloques, sino que además nacieron nuevas criptomonedas que comparten el mismo origen.

3.4.3) Bifurcaciones de software

Las bifurcaciones de software o "soft forks" consisten en una actualización de software que es compatible con la versión anterior. En este caso, la comunidad minera realiza y acepta cambios de software, pero el cambio no provoca un ajuste subyacente que no sea compatible con bloques extraídos anteriormente.

Este cambio se ve reflejado en la “Versión de Software” que se encuentra estampada en el bloque, indicando el número de versión de software que generó el bloque en cuestión. Un “soft fork” tiene tres variables posibles:

- Todos los mineros están de acuerdo, y la bifurcación no es realmente una bifurcación, solo un cambio de software

- La mayoría de los mineros está de acuerdo, la nueva bifurcación se adopta y la bifurcación vieja muere lentamente.

- La mayoría de los mineros no está de acuerdo y la nueva bifurcación muere.

4. TRANSACCIÓN DE CRIPTOACTIVOS

Las investigaciones de actividades delictivas vinculadas con criptoactivos puede resultar compleja, dado que muchos casos podrían estar vinculados con compras realizadas o fondos transferidos a través de la cadena de bloques, por lo que resulta vital comprender con precisión cómo se preparan, transmiten, procesan y almacenan las transacciones.

4.1. Operaciones convencionales y operaciones con criptoactivos

Para una mejor comprensión del funcionamiento de las transacciones en un sistema de cadena de bloques como Bitcoin, resulta propicio aclarar que se aparta considerablemente de la lógica inherente a las transacciones convencionales.

En efecto, las transacciones de dinero tal y como las conocemos tienen un punto en común: el movimiento de moneda del dueño de esa moneda a otro individuo, es decir, la tradición.

Tomemos como ejemplo la transacción en efectivo: una persona se sienta en un bar y toma un café, luego busca en su billetera y extrae $ 350. Al entregar los billetes al camarero, transfiere físicamente la moneda a un nuevo propietario.

Sería lo mismo con una transacción electrónica. Supongamos que esta persona elige pagar a su café con una tarjeta bancaria. La transacción es idéntica, excepto que no ve el movimiento del dinero. Detrás de escena, el dinero es «tomado» o debitado de su cuenta y «dado» o acreditado a la cuenta del bar. En ambos ejemplos, la transacción está controlada y respaldada por una autoridad central.

Independientemente, como ya mencionamos, la moneda está controlada centralmente por el Estado y se denomina dinero fiduciario, término que proviene del latín y refiere a «que se haga». Esto también significa que, si la misma persona quiere un café en París, no puede simplemente darle al camarero un billete de $ 350, sino que se tiene que gestionar una transacción que permita el cambio de moneda de pesos argentinos a euros, y recién luego puede pagar su café de forma tal que el banco local lo acepte. Esto es costoso ya que siempre se pierde dinero en una transacción de divisas en tarifas y tipos de cambio.

Con los criptoactivos, no existe tal problema porque no hay una autoridad central con la que tratar. La existencia de un registro distribuido implica que no hay un control superior y los cambios en la cadena de bloques solo se llevan a cabo por consenso de los usuarios, siendo esta una de las razones por la cual esta tecnología es adoptada a nivel global.

Eso sin mencionar el caso de transferencias internacionales, donde existen infinidad de restricciones y los costos varían según montos máximos y mínimos establecidos por las diferentes entidades bancarias.

4.2. Direcciones y claves criptográficas público/privada

La tecnología detrás de los criptoactivos garantiza, en cierta medida, que cada unidad o fracción de la misma sólo pueda ser transmitida por quien la posee y nunca más de una vez. Para ello, cada usuario que participa en la red posee una dirección en la que se reciben los valores. Luego, para poder disponer de ellos, debe "firmar" la operación con una llave criptográfica asociada a la misma.

La dirección[16] actúa como punto receptor del pago, y consiste en un código alfanumérico[17] que se genera como resultado de la aplicación de operaciones estandarizadas –entre las que se incluyen funciones "hash"– sobre una clave pública, la que se obtiene, a su vez, por medio de otra serie de cálculos preestablecidos[18] y ejecutados sobre una clave privada, la que es generada por el usuario o por la plataforma utilizada por aquél a los fines de operar en la red[19].

Es decir que a partir de la clave privada es posible calcular la clave pública y, seguidamente, la dirección que le será provista luego a terceros para que envíen los pagos que se pretendan percibir. Sin embargo, no será posible realizar el camino inverso y obtener, a partir de una dirección, la clave privada.

El carácter secreto de dicha clave responde a su función, ya que es indispensable para "firmar" la operación y autorizar, de ese modo, el traspaso de las criptomonedas o "tokens" a otra dirección. En otras palabras, la clave privada es la "llave" que le permite al usuario disponer de sus fondos, por lo que deberá ser resguardada de manera segura para impedir que un tercero se apodere de los criptoactivos.

16. Pese a ser una denominación técnica, en ocasiones se hace alusión a las direcciones utilizando el término "billetera virtual" o simplemente "billetera". Veremos más adelante que al término "billetera" se le otorga un alcance diferente, por lo que se desaconseja su uso para referirnos a las direcciones.

17. El formato de direcciones más tradicional en Bitcoin posee una extensión que, en principio, varía entre los 26 y 35 caracteres (direcciones en formato "Base58check"), y comienzan con los dígitos 1 o 3. Existe a su vez otro tipo de direcciones (formato "Bech32") cuya extensión puede alcanzar los 90 caracteres. En este último caso, las direcciones iniciaran con la seguidilla de caracteres bc1q o bc1p.

18. En concreto, en el caso de Bitcoin, se realizan las operaciones establecidas por el Algoritmo de Firma Digital de Curva Elíptica o ECDSA –acrónimo de *Elliptic Curve Digital Signature Algorithm*–, que constituye la base del sistema de criptografía asimétrica del que se vale la plataforma.

19. La clave privada es un código de 256 bits. Cualquier persona puede generar a una o tantas claves privadas como desee, en tanto prácticamente cualquier código que cumpla con esas características es, potencialmente, una clave privada funcional. Existen páginas y aplicaciones generadoras de claves privadas que simplifican su creación y la obtención de sus respectivas direcciones, por ejemplo https://www.bitaddress.org y https://vanitygen.net/.

4.3. Mecanismo de las transacciones

Las transacciones –denominadas habitualmente como TX– constituyen una parte esencial e indispensable en el mecanismo de intercambio de criptoactivos. Estas representan la columna vertebral de este complejo y eficiente sistema criptográfico.

Básicamente, una transacción es un envío o transferencia de un determinado valor entre dos partes. En Bitcoin, por ejemplo, las transacciones constituyen el envío de unidades o porciones de este criptoactivo[20] entre personas que utilizan la red mediante sus respectivas direcciones o claves públicas. Pero en realidad, estas transacciones no son más que un constante flujo de información, representado mediante los registros almacenados en la "blockchain" de Bitcoin. Cabe destacar que el mismo principio se aplica también al resto de los criptoactivos, como por ejemplo Ethereum.

4.3.1) Tipos de transacciones en la red Bitcoin

Continuando con el ejemplo de Bitcoin, existen tres tipos principales de transacciones:

- P2PKH o pago a hash de clave pública; esto es lo que podría considerarse una transacción estándar en Bitcoin, con una dirección de clave pública transfiriendo valor a otra dirección. La gran mayoría de las transacciones en la cadena de bloques de Bitcoin son P2PKH. Las direcciones correspondientes a este tipo de transacciones utilizan el formato "Base58check" y comienzan con el dígito "1".

- P2SH o pago de hash mediante instrucciones; en este caso las transacciones "multisignature" o de firma múltiple[21] son el principal ejemplo de una transacción P2SH, aunque no es su único uso. La dirección que emite el pago deberá cumplir con una serie de requisitos preestablecidos mediante comandos que deberán cumplirse antes que el valor pueda transferirse. Por ejemplo, la secuencia de comandos podría requerir la intervención de varias claves privadas, como en una transacción de firma múltiple, una contraseña o cualquier requisito que se pueda incorporar en la secuencia de instrucciones codificadas. Las direcciones correspondientes a este tipo de transacciones utilizan el mismo formato que las anteriores, pero comienzan con el dígito "3".

4.3.2) Actualizaciones en la cadena de bloques de BTC

Cabe destacar que a medida que los criptoactivos se hicieron populares, especialmente Bitcoin,

20. Un Bitcoin es divisible en 100.000.000 de "céntimos" llamados Satoshis, permitiendo reflejar saldos o transacciones de hasta ocho decimales. Por tanto, la unidad de valor o fracción mínima de un bitcoin sería 0,00000001

21. Este tipo de transacciones requieren de más de una clave privada para que los fondos habidos en una dirección puedan ser transferidos, o pueden diseñarse para que los fondos puedan ser transferidos indistintamente por cualquiera de las claves privadas establecidas al configurarla. Esto puede ser útil cuando se requiere que varios directivos de una empresa u organismo aprueben un pago.

surgieron ciertas limitaciones y riesgos de seguridad debido a la estructura mediante la cual funcionaban sus transacciones. En tal sentido, una de las mejoras más importantes de la cadena de bloques de Bitcoin fue la incorporación en el año 2017 de las transacciones en formato de testigo segregado o "Segregated Witness" –"Segwit"–, mediante una bifurcación de software.

Esta mejora impactó de diferentes maneras, en primer lugar, resolvió el problema de maleabilidad de las transacciones y por otro lado otorgó escalabilidad a la red Bitcoin. Este tipo de transacciones pueden ser identificadas como pago a hash de clave pública –P2WPKH– o pago de hash mediante instrucciones mediante testigos segregados –P2WSH–. Las direcciones utilizadas en este tipo de transacciones poseen formato "Bech32" y se identifican por el prefijo "bc1q".

Otra de las mejoras realizadas sobre la cadena de bloques de Bitcoin fue "Taproot". Esta actualización tuvo lugar en el año 2021 y tiene como finalidad realizar mejoras en la privacidad, eficiencia y costo de las transacciones, al incorporar nuevas funcionalidades para las transacciones de pago de hash mediante instrucciones. Por su parte, las direcciones correspondientes a este tipo de transacciones comparten el formato con las anteriores, pero comienzan con la sucesión de caracteres "bc1p".

4.3.3) Posibles estados de las transacciones en la red Bitcoin

Si bien para los usuarios las transacciones o transferencias de fondos desde sus direcciones se realizan de forma "transparente", desde el punto de vista técnico se realizan una serie de pasos adicionales que garantizan las operaciones y su asiento en el libro maestro que denominamos "blockchain".

Cada transacción en la cadena de bloques de Bitcoin consta de entradas (lo que se envió) y salidas (lo que se recibió) firmadas criptográficamente, validadas y confirmadas por la red de nodos.

Ahora bien, una transacción puede encontrarse en uno de los siguientes estados:

- "Spent State" o Estado gastado: en estos casos todo el valor o monto disponible en una

Un elemento crítico de una dirección es que su propietario no puede gastar o transferir solo parte de ella. Por ejemplo, si una dirección tiene 5 Bitcoins y propietario desea "comprar" algo por el valor de 1 Bitcoin, este deberá realizar una transferencia equivalente a todo su saldo, es decir los 5 Bitcoins completos en esa transacción y recibir el resto como cambio o vuelto en una nueva dirección -lo que ocurre en general- o en una ya utilizada. La situación planteada presenta dos términos muy importantes sobre los que ya hablamos previamente, "outputs" o salidas e "inputs" o entradas.

Como su nombre lo indica, los "outputs" equivalen a transferencias de salida, mientras que los "inputs" equivalen a transferencias de entrada, del mismo modo, en el caso de las UTXO una transacción de entrada se vincula directamente con la salida de una transacción anterior.

El conjunto de entradas y salidas, la cantidad de criptoactivos a enviar y firmas criptográficas, dan como resultado un "hash" de transacción, normalmente llamado "identificador hash", "Hash ID" o "TXID".

5. MINERÍA

Las operaciones con Bitcoin, dijimos, son comunicadas a toda la red por medio de los nodos conectados a través de internet que, además, verifican su validez –es decir, que posean una firma válida y que las direcciones cuenten con los activos que se pretende transferir–. Tras ello, son incorporadas por un tipo específico de nodo validador –junto a otras tantas operaciones– en un nuevo bloque de datos, lo que se comunica a toda la red para que se actualice la base de datos almacenada en cada uno de los nodos. Los procesos descriptos constituyen la base del modelo de consenso propuesto por la generalidad de los criptoactivos que cuentan con su propia cadena de bloques.

5.1. Mineros

En el caso de Bitcoin, al nodo validador que aspira a cumplir dicha labor se lo denomina "minero". Los "mineros" no son un actor esencial para el funcionamiento de cualquier criptomoneda, sino solo para aquellas que adoptan el sistema de validación por "prueba de trabajo" (conocido como "PoW", acrónimo de "proof of work"). El "minero", en estos casos, compite con otros "mineros" para determinar quién se hace acreedor del derecho a incorporar un nuevo bloque a la cadena. Se trata de una competencia que le exige a cada participante la realización de un gran volumen de operaciones matemáticas.

El objetivo para cada uno de ellos, en el caso de Bitcoin, es ser el primero que, aplicando una función hash al conjunto de datos que contendrá el nuevo bloque proyectado[22], arribe a un resultado cuyo valor sea inferior al piso fijado por el sistema, dotándolo así de validez. Para ello, al conjunto de datos que conformarán el bloque, el minero debe adicionarle una variable, que en este caso será el número denominado "nonce" sobre el cual ya hablamos anteriormente al describir la estructura de un bloque de la "blockchain".

El sistema modifica frecuentemente el grado de dificultad del objetivo –es decir, el valor por debajo del cual deberá hallarse el resultado del "hash"– de modo tal que, teniendo en cuenta la cantidad de poder de "minado"[23] que se esté destinando a la red en un momento dado, el hallazgo del objetivo por parte de alguno de los participantes demore, aproximadamente, diez minutos.

---

22. Cada "minero" proyecta por sí mismo un bloque, incorporando en aquél un conjunto de operaciones efectuadas por usuarios que no han sido validadas aún, es decir, operaciones que se encuentran a la espera de ser incorporadas en un nuevo bloque que sea incorporado a la cadena.

23. La referencia utilizada para medir el poder de cómputo específico para la labor de "minería" es el "hash rate" –o tasa de hash– sobre una unidad de tiempo, es decir, cuántas de estas operaciones hash puede llevar a cabo un dispositivo en un determinado lapso.

5.2. Rentabilidad y tipos de mineros

El "minado", naturalmente, tiene un costo. No todos los procesadores computacionales son adecuados para el trabajo, e incluso aquellos que sirven para "minar" un tipo de activo pueden no ser idóneos o convenientes para otros. A su vez, los procesadores más efectivos suelen ser también más caros, requieren de mantenimiento, consumen una gran cantidad de energía eléctrica y producen altas temperaturas que deben ser disipadas para que los componentes funcionen adecuadamente. La rentabilidad de la "minería" dependerá, entonces, de la minimización de estos costos[24].

Algunas criptomonedas como Bitcoin, debido a la cantidad de poder de procesamiento que fue incorporándose a la red y al inherente aumento de la dificultad, solo pueden "minarse" de manera rentable con un equipamiento específico al que se denomina ASIC[25]. Otras criptomonedas, sin embargo, pueden ser minadas mediante placas del tipo GPU[26], más económicas que las anteriores, y aun así generar ciertas ganancias.

Es posible "minar" ciertos tipos de criptomonedas mediante equipos con menor poder de cómputo, constituidos con otro tipo de placas, e incluso, por medio de computadoras como las que se encuentran en la mayoría de los hogares, celulares, tablets, etc. Sin embargo, no suele ser rentable cuando se tienen en cuenta los costos descriptos anteriormente, aunque ello dependerá finalmente de otras variables como el valor en el mercado del activo en cuestión y su sistema de recompensas.

Algo similar ocurre con la "minería" en la "nube", en la que el interesado contrata el poder de cómputo de un tercero para "minar" en una o varias plataformas. En estos casos, en el valor del servicio se verá reflejada –además de los costos enunciados anteriormente– la ventaja patrimonial que obtendrá el administrador de la infraestructura por brindarlo, lo que naturalmente atenta contra la rentabilidad del negocio para el contratante.

5.3. Prueba de trabajo Vs Prueba de participación

Existe un gran número de alternativas al sistema de validación "PoW", una de ellas es el sistema de "Prueba de participación" –conocido como "PoS" o *"proof of stake"*, recientemente implementado,

---

24. Tal es así que los emprendimientos de minería más importantes suelen encontrarse en países donde la energía eléctrica es más barata y/o en regiones con bajas temperaturas.

25. Acrónimo de "Application–Specific Integrated Circuit", o Circuito integrado de Aplicación Específica, se trata de procesadores diseñados para una finalidad particular, en el caso, para el minado en la red Bitcoin.

26. Placas de procesamiento gráfico, como las que se utilizan en las computadoras diseñadas para jugar videojuegos o correr programas que requieren de muchos recursos para poder elaborar gráficos complejos, como por ejemplo imágenes en 3D.

sin ir más lejos, en la red Ethereum[27]–. Aquí, los pretensos validadores de bloques deben poner a disposición una cantidad de activos, que operan como una suerte de garantía. Seguidamente, el sistema selecciona al azar, entre estos usuarios, a aquél que tendrá la facultad de incorporar el siguiente bloque **válido a la cadena**. Cuanto mayor sea el monto dispuesto, más altas serán sus probabilidades de ser designado como validador.

La diferencia sustancial con respecto al sistema anterior radica en que aquí los usuarios no compiten entre sí mediante el despliegue de su poder computacional, sino mediante el volumen de capital que se encuentran en condiciones de consignar, lo que reduce drásticamente el gasto en energía e infraestructura informática.

Aclarado esto, resta mencionar que aquellos actores de las respectivas redes que se ven beneficiados con el derecho a incorporar un nuevo bloque a la cadena suelen recibir, a modo de contraprestación o "premio", una suma de criptoactivos –ello al margen de las tarifas o "fees" asignadas por los usuarios en cada una de las transacciones incorporadas al bloque–. Dicho proceder es utilizado por algunas de las plataformas, como por ejemplo Bitcoin, para resolver los aspectos relativos a la emisión de nuevas unidades de valor[28].

5.4. Pooles de minería

En efecto, en la red Bitcoin los "mineros" perciben, por cada bloque procesado e incorporado a la cadena, un valor compuesto por la suma de las comisiones fijadas por los usuarios en las respectivas operaciones incorporadas al bloque y, además, una cantidad de bitcoins emitidos por el sistema, siendo éste el r**é**dito principal que obtienen hoy en día por su labor.

Si bien podría parecer en líneas generales una práctica rentable, no debe perderse de vista que las probabilidades de ganarse ese derecho son sumamente bajas. Aun cuando Bitcoin incorpora más de 50.000 bloques nuevos cada año, existen millones de dispositivos interconectados que compiten, constantemente, para hacerse acreedores del derecho a agregarlos. En otras palabras, es posible "minar" durante años con un dispositivo y aun así no obtener ninguna ganancia.

Dicho escenario dio lugar a la creación de "pooles" de minado. Se trata de una metodología de trabajo en el que los actores despliegan su poder de cómputo ya no individualmente, sino en sociedad con otros actores interesados. De ese modo, si alguno de los miembros del grupo logra dar con el valor

27. La prueba de participación es un tipo de mecanismo de consenso que usan las redes de "blockchain" para lograr consensos distribuidos, un claro ejemplo de ello es la implementación de este tipo de sistema de validación en la red Ethereum (https://ethereum.org/es/developers/docs/consensus-mechanisms/pos/).

28. La forma en que se dosifica la emisión varía de una criptomoneda a otra. En el caso de Bitcoin, se comenzó en el año 2009 con una emisión de 50 bitcoins por cada nuevo bloque "minado", aunque cada cuatro años aproximadamente –el tiempo estimado que le toma a la red incorporar 210.000 bloques nuevos a la cadena– esa emisión es reducida a la mitad. Al día de la fecha, el sistema emite por cada bloque nuevo un total de 6.25 bitcoins.

requerido por el sistema, las ganancias se distribuyen entre todos, prorrateadas en función del poder de cómputo que cada uno destinó al "minado" en esa ocasión. Naturalmente, los pagos que percibirán los participantes serán de un valor menor –en comparación con aquél que logra validar un bloque por su propia cuenta–, pero las probabilidades de obtener un rédito aumentarán considerablemente.

El "pool" puede implementarse de diferentes maneras, aunque, en líneas generales, suelen tener un administrador o un nodo en el que se centraliza la coordinación de la labor, la administración y la distribución de las ganancias, entre otros pormenores. Es a dicho nodo que los participantes deben comunicarle los resultados de las operaciones que realizan con sus dispositivos, para que desde allí se comunique luego, a la red Bitcoin –o a la que corresponda, dependiendo de cuál sea el activo "minado"– el hallazgo del nuevo bloque válido cuya incorporación se propone. Otros "pooles", no obstante, optan por abonarles a los usuarios un precio por el volumen de cómputo que suministran, sin importar la frecuencia con la que logre "minarse" un nuevo bloque.

Los miembros del "pool" de minado deberán identificarse de algún modo ante el nodo que centraliza la labor, para que éste pueda constatar cuánto poder de cómputo dedicó cada uno y, de este modo, asignarle a cada "minero" la proporción de la ganancia obtenida a raíz de la incorporación del nuevo bloque a la cadena o el precio acordado por el poder de cómputo suministrado.

5.5. Minería y Tokens

Repárese que a lo largo del presente se hizo alusión a Bitcoin o a la subespecie identificada como criptomonedas. La exclusión de los "tokens" responde a que aquéllos no se erigen como plataformas autónomas[29], a diferencia de las anteriores, y por ello, tal como veremos, su base de datos no se construye del mismo modo.

Las transacciones realizadas por medio de "tokens" se procesan de acuerdo a las condiciones establecidas en el contrato electrónico correspondiente, pero para ello, los comandos contenidos en él deben ejecutarse. Ello requiere –como ocurre con cualquier programa informático– de cierto poder de cómputo. Pues bien, tal poder será provisto por los nodos designados a tal efecto dentro de la plataforma sobre la cual se montó el contrato o, en otras palabras, por los "mineros" o validadores de aquella red, aunque no de manera exclusiva, en tanto éstos procesaran también los comandos de otros contratos existentes.

Aun así, ciertos desarrollos de esta naturaleza toman algunos de los aspectos propios de estos mecanismos y los adaptan para resolver, por ejemplo, cuestiones como la emisión de nuevas unidades

29. Los "tokens" –como ya dijimos– son contratos electrónicos –que, en esencia, son programas informáticos– montados dentro de otra estructura preexistente que admite la inserción de este tipo de elementos, por ejemplo, la plataforma "Ethereum".

de valor.

6. BILLETERAS VIRTUALES

Dada la complejidad de almacenar y administrar de manera segura las direcciones y sus llaves privadas, existen algunos desarrollos que facilitan su uso y resguardo. A este tipo de herramientas se las denomina “billeteras virtuales” o “monederos virtuales” y podemos encontrarnos con una gran variedad de implementaciones.

Una billetera virtual no almacena criptoactivos, pero sí hará referencia a cualquier transacción en la cadena de bloques que se pueda vincular con las claves privadas gestionadas por intermedio de esta.

Ahora bien, cabe distinguir las billeteras virtuales de las aplicaciones provistas por diferentes plataformas privadas que proveen servicios de arbitraje y/o compraventa de criptoactivos, conocidas comúnmente como “Exchanges”.

En estos casos, las plataformas son quienes administran los activos y registran, en sus bases de datos, los movimientos de las cuentas de sus usuarios. Para realizar una operación, el usuario debe solicitárselo a la plataforma a través de alguno de los medios provistos a tal efecto, por lo general, a través de una aplicación o plataforma web.

En cualquier caso, tanto el usuario particular como la plataforma que administra los criptoactivos de múltiples clientes podrán valerse de este tipo de desarrollos para almacenar sus direcciones y claves privadas, como así también, para perfeccionar sus transacciones.

6.1. Tipos de billeteras

Para cada criptoactivo, existen numerosos formatos de billeteras que pueden funcionar en diferentes tipos de dispositivos –computadoras de escritorio, teléfonos móviles y tabletas– y/o sistemas operativos –Linux, Windows, MacOs, Android, iOS–.

Nos encontramos también con programas que resguardan toda la información localmente, es decir, en el dispositivo en el cual se utilizan, y otras plataformas en las que los usuarios deben crearse una cuenta, con un nombre de usuario y una contraseña, y la información en cuestión es almacenada en los servidores de la empresa que brinda el servicio.

Mientras que en el primer caso se prioriza la privacidad de la información, en el segundo, se pondera la accesibilidad, ya que, si bien se encontrará en manos de terceros, será accesible desde cualquier dispositivo en forma indistinta.

6.1.1) Billeteras por software

En este apartado se pueden señalar tres tipos:

- Billetera de nodo completo o *"full node"*: en estos casos se descarga localmente toda la cadena de bloques. Las transacciones realizadas pueden procesarse y verificarse localmente para luego transmitirse a sus pares.

- Billetera de nodo ligero o *"thin node"*: este cliente se conecta a otro nodo completo para el procesamiento de transacciones.

- Billetera en línea u *"online wallet"*: este es un monedero que solo existe en un sitio web; los datos de la transacción generalmente no se sincronizan con un cliente local.

6.1.2) Billeteras por hardware

Las billeteras de hardware son dispositivos físicos que almacenan claves privadas y otros datos del usuario, como por ejemplo el saldo de su cuenta.

Estos dispositivos son generalmente muy seguros, por lo que, si se llegara a incautar uno de ellos, posiblemente sea necesaria la cooperación del propietario para desbloquearla. Sin embargo, existen ciertas maniobras de recuperación en caso de pérdida de PIN de acceso o extravío del dispositivo. Comprender estos pasos de recuperación, posibilita obtener acceso a su contenido sin necesidad de contar con acceso físico al dispositivo o mediante su respectivo PIN.

6.1.3) Billeteras frías o almacenamiento en frío

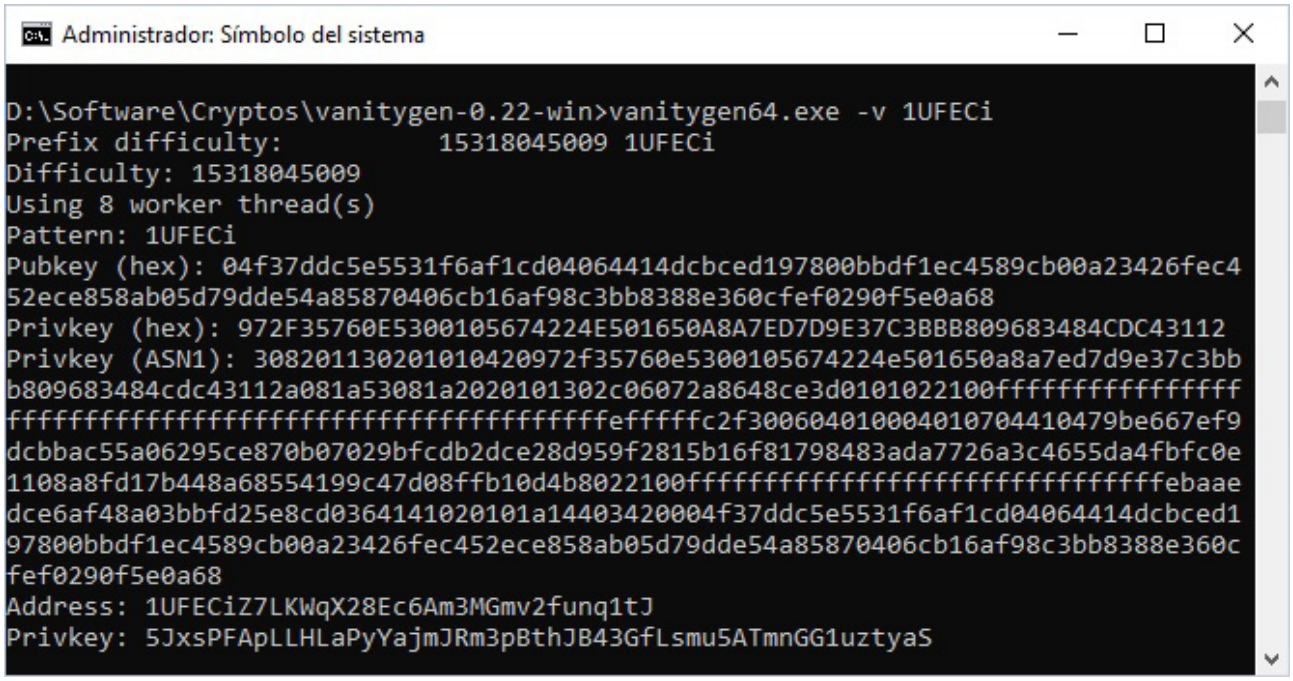
Como expusimos anteriormente, una billetera no tiene nada que ver con el almacenamiento de criptoactivos e incluso realizar una copia de seguridad de una billetera es solo una manera de mantener el registro y gestión de claves privadas.

Esto significa que simplemente se podría anotar la clave privada en una agenda y guardarla en un cajón. Este es un buen ejemplo de una billetera fría, es decir una clave privada escrita en una hoja de papel. Sin embargo, el almacenamiento en frío realmente define cualquier clave que se mantiene fuera de línea, y esto podría estar en una llave USB, una nota de papel o una billetera de hardware.

Del mismo modo, es importante destacar que, si bien una clave privada puede mantenerse fuera de línea y debe importarse a una billetera para poder transferir fondos, la billetera fuera de línea aún puede recibir transacciones de cualquier remitente.

Tal circunstancia se debe a que en realidad la billetera nunca recibe los criptoactivos, sino que solo hace referencia a la dirección en la cadena de bloques. Por lo tanto, una dirección y su clave privada o una copia de seguridad como una semilla mnemotécnica[30] almacenada en una hoja de papel en una caja fuerte aún pueden recibir transacciones mientras se encuentran completamente fuera de línea.

Esto es extremadamente seguro porque siempre que no se necesite mover los fondos recibidos en la dirección de la clave pública, la clave privada nunca se vinculará con una billetera o dispositivo.



30. Una regla mnemotécnica utiliza oraciones cortas y fáciles de recordar que ayudan a relacionar y memorizar palabras.

Los ejemplos ilustrados corresponden a diferentes aplicaciones para generar billeteras frías mediante la aplicación "Vanity Gen" y el sitio web "Wallet Generator"[31].

6.2. Cómo se almacenan las claves

Las billeteras almacenan claves de varias maneras, definiendo la forma en que se crean las claves públicas a partir de una o varias claves privadas. Estos métodos se dividen en tres categorías principales:

6.2.1) Billeteras No Deterministas

También conocidas como tipo 0, las claves no deterministas se almacenan en una lista simple de pares de claves públicas/privadas. Esto también se conoce como JBOK –solo un manojo de llaves o "just bunch of keys"–.

Este método implica varios conjuntos de claves para administrar, especialmente si es utilizada una nueva dirección para cada transacción[32]. De forma directamente proporcional, esto también significa que existe una gran cantidad de datos para respaldar y mantener seguros.

6.2.2) Billeteras Deterministas

Las billeteras deterministas también se conocen como billeteras tipo 1 y parten de una "frase semilla" o "seed phrase", un conjunto de palabras[33] que, por medio de ciertas operaciones previstas en un protocolo, se traducen en un código que es utilizado como insumo para generar un sinfín de claves públicas/privadas. Existen múltiples programas y plataformas que permiten utilizar este tipo de billeteras y, sin importar cuál se utilice, en la medida que uno ingrese las mismas palabras en el mismo orden, podrá acceder en cada oportunidad a sus direcciones y claves públicas/privadas.

---

31. El ejemplo propuesto fue tomado de https://walletgenerator.net/.

32. En el ecosistema de los criptoactivos y, en particular, en aquéllos que se rigen por el sistema de transacciones UTXO –a diferencia de, por ejemplo, Ethereum–, se aconseja evitar, en la medida de lo posible, el uso de una misma dirección en más de una operación, en aras de velar por la seguridad y la privacidad de los usuarios. Dicha práctica ha sido ampliamente receptada e implementada por la mayoría de las plataformas y aplicaciones que proveen servicios de "billetera virtual" para usuarios particulares, por lo que las operaciones que se realizan por ese medio suelen adecuarse al proceder descripto, lo que implica que cuando el usuario quiera recibir criptomonedas por parte de un tercero, la plataforma o aplicación generará –en la mayoría de los casos– una nueva dirección para que sea compartida con la persona que deba realizar el pago. Del mismo modo, cuando se pretenda transferir a un tercero una cantidad de criptoactivos inferior al valor total almacenado en la dirección de origen, la aplicación o plataforma procurará que el remanente se envíe a una dirección nueva –a la que se suele denominar "dirección de cambio"–, para así "descartar" la dirección originaria. Sin embargo, la situación varía en relación a las personas o empresas cuyo negocio gira en torno al intercambio de criptomonedas, o que simplemente admiten pagos mediante las mismas. En estos casos, puede resultar conveniente contar con una dirección a la que los clientes sepan que pueden transferir sus fondos cada vez que necesiten realizar un pago, sin necesidad de verse obligados a constatar, previo a cada operación, cuál es la nueva dirección en la que la empresa querrá recibir la transferencia en cuestión. Es por ello que, cuando se advierte una multiplicidad de operaciones asociadas a una misma dirección, es dable sospechar que podría pertenecer a un comerciante o proveedor de servicios.

33. No se trata de cualquier palabra, las mismas deben ser extraídas de un diccionario preestablecido en el protocolo –existen diccionarios en diferentes idiomas, cada uno con un total de 2048 palabras–. Habitualmente se utilizan doce palabras –lo que conforma una clave de 128 bits–, pero algunas plataformas generan "frases semilla" con un número menor o mayor, por ejemplo, veinticuatro palabras –256 bits– que, como es de suponer, será más segura. A su vez, este sistema admite la utilización de una "palabra extra", en rigor, una contraseña generada por el usuario. Pueden encontrarse los diccionarios y mayores detalles del protocolo en https://github.com/bitcoin/bips/tree/master/bip-0039.

6.2.3) Billeteras Deterministas Jerárquicas

También conocido como "billeteras HD"–"Hierarchical Deterministic"–, este es el protocolo de billetera más actualizado en uso.

Al igual que con las billeteras deterministas estándar, todas las claves privadas se derivan de una sola semilla, pero las claves en una billetera HD pueden generar sus propias claves privadas y públicas en una estructura de árbol jerárquica. Una vez más, la semilla se puede respaldar y la estructura completa del árbol se puede recuperar a partir de esta copia de respaldo.

7. ASPECTOS INVESTIGATIVOS

Es importante destacar que si bien las transacciones en la red Bitcoin –y en un gran número de plataformas de criptoactivos– son totalmente públicas, la mencionada cadena de bloques solamente revela las direcciones que han participado de cada operación validada por la red, en las que se enlazan los valores transferidos, así como también la fecha y hora en la que tuvieron lugar.

Por medio de la Resolución de la Unidad de Información Financiera (UIF) n° 300/2014[34], del 4 de julio de 2014, el organismo encargado del análisis, tratamiento y transmisión de información de inteligencia financiera para prevenir el lavado de dinero y el financiamiento del terrorismo, se emitieron una serie de medidas tendientes a mitigar los riesgos que implica el uso de los activos virtuales, siendo algunos de los más significativos el anonimato, así como la dificultad de la trazabilidad nominativa de las operaciones y las vulnerabilidades que pueden ser aprovechadas con fines criminales.

Entre esas medidas, se les requirió a los Sujetos Obligados por la ley 25.246[35] y sus modificatorias una especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales, que establezcan un seguimiento reforzado respecto de estas operaciones, evaluando que se ajusten al perfil del cliente que las realiza, de conformidad con la política de conocimiento del cliente que hayan implementado, e impone a los sujetos obligados a que reporten como operaciones sospechosas a todas las operaciones efectuadas con monedas virtuales.

Si bien es cierto que estas medidas implicaron un fortalecimiento en el control de las operaciones con este tipo de activos, tampoco debe perderse de vista que las empresas o plataformas que funcionan como "Exchanges" aún no se encuentran comprendidas por la nómina de sujetos obligados a ejercer el control y reporte de operaciones sospechosas de lavado de dinero y financiamiento del terrorismo. Por lo tanto, aunque algunas de esas empresas voluntariamente estén llevando adelante una política para mitigar los posibles riesgos de verse implicadas en transacciones sospechadas mediante medidas de debida diligencia y conocimiento de clientes, al no estar alcanzadas expresamente por el régimen administrativo, aquel control es más laxo que la supervisión rigurosa que la ley y las reglamentaciones específicas prevén para las entidades del sector financiero o las de las actividades profesionales no financieras designadas (APNFDs).

7.1. Pseudoanonimato

En lo que respecta a la identidad de los usuarios detrás de las direcciones involucradas, la cadena

34. http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm
35. Enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del artículo 20 de la Ley

de bloques no provee información alguna. No se consignan en ella nombres, direcciones, teléfonos, correos electrónicos, simplemente no es necesario brindar esa información para realizar las operaciones y, el protocolo que determina su funcionamiento, no prevé siquiera la inserción de esos datos en la cadena de bloques. Tampoco se almacenan en ella las direcciones IP[36] de conexión que se utilizaron para efectuar las transferencias entre ambos extremos.

En efecto, si bien los nodos participantes podrían establecer desde qué dirección IP proviene la comunicación de una nueva transacción, por la manera en que se comunican las operaciones concretadas dentro de la red –aquí hay que recordar que no existe un nodo o entidad central que intervenga en todas ellas, sino que son los propios operadores quienes procesan, transmiten y retransmiten las transacciones efectuadas–, resulta sumamente difícil identificar, de manera fehaciente, cuál fue el nodo integrante de la red que comunicó inicialmente cada una de las operaciones.

Sin perjuicio de lo señalado, no es correcto afirmar que las operaciones realizadas con criptoactivos quedan sepultadas sin más en el anonimato, aunque en razón de sus características, es necesario recurrir a otros medios –más allá de la mera observación de la base de datos– para poder individualizar a las personas que están detrás del manejo de cada dirección.

7.2. Etiquetado y agrupado de direcciones

Sin ir más lejos, es posible verificar, a través de determinadas herramientas de acceso público, si las direcciones involucradas en una determinada maniobra –u otras direcciones con las que éstas celebraron alguna operación antes o después– fueron publicadas en algún sitio, en algún perfil, o si se encuentran asociadas a una casa de cambio virtual, a una plataforma que brinde un servicio de "billetera virtual" u a otra compañía que brinde servicios relacionados con los criptoactivos.

Usualmente, las herramientas de análisis de las bases de datos de los diferentes criptoactivos utilizan, como punto de partida para "desanonimizar" las operaciones –es decir, para identificar a las personas detrás de una dirección–, el "etiquetado" de las direcciones identificadas.

Ello se logra a partir de la información recolectada mediante la celebración de operaciones con diferentes personas o plataformas, o por medio del relevamiento de diferentes fuentes abiertas de información, por ejemplo, empresas que publican abiertamente en sus sitios web las direcciones que

36. La dirección IP identifica una conexión a internet desde un dispositivo (computadora de escritorio o portátil, celular, tableta o cualquier otro aparato con conexión a internet –televisores inteligentes, heladeras –esto es lo que se llama "internet en las cosas" o IoT–) en un momento determinado. Esas direcciones IP, que son únicas a través de toda la red de redes, están formadas por un grupo de cuatro segmentos (ej. 200.55.243.205, el número mínimo es 0.0.0.0. y el máximo 255.255.255.255.) y se encuentran distribuidas mundialmente en bloques y son asignadas a los clientes por proveedores del servicio de internet –ISP– (ejemplos de ISP en nuestro país son "Speedy" –de Telefónica de Argentina S.A.–, y "Flow" –de Telecom Argentina S.A.). En la actualidad este protocolo de direcciones IP, denominado IPv4 se está reemplazando por uno nuevo, denominado IPv6 ya que límite en el número de direcciones de red admisibles en el IPv4 está empezando a restringir el crecimiento de Internet y su uso. El nuevo protocolo admite direcciones IP mucho más largas y alfanuméricas, de forma tal que cada vez más dispositivos conectados a internet podrán tener una dirección IP asignada exclusivamente a ellos.

utilizan, usuarios que las plasman en foros, redes sociales, etc.

A su vez, la labor mencionada suele complementarse con una técnica de "agrupado", que consiste en adjudicarle todas las direcciones de origen utilizadas en el marco de una única transacción a una única persona. La lógica detrás de ello consiste en que, quien realiza una transferencia de fondos, debe poseer el control –es decir, las claves privadas– de todas las direcciones de origen. Así, al identificar alguna de esas direcciones en una nueva operación, será posible afirmar que las demás direcciones de origen pertenecen, también, a dicho usuario. Sin embargo, ambos sistemas son falibles.

El valor probatorio del "etiquetado" será tan sólido como lo sea la fuente de información utilizada, la que en muchos de los casos –especialmente en las plataformas gratuitas– se desconoce. A su vez, se utilizan miles de direcciones nuevas cada día y otras tantas dejan de utilizarse a un ritmo similar, por lo que la base de datos debe ser actualizada de manera constante.

Por otra parte, la premisa detrás del "agrupado" puede ser quebrantada por los usuarios. Existen procedimientos que permiten enviar criptoactivos desde distintas direcciones a múltiples direcciones de destino, en el marco de una misma operación, aunque utilizando direcciones de origen de diferentes usuarios, sin necesidad de que los sujetos involucrados compartan entre sí sus respectivas claves privadas.

7.3. Trazabilidad de las transacciones

Mediante determinadas herramientas de acceso público y fuentes abiertas de información, resulta posible verificar si las direcciones involucradas en una determinada maniobra –u otras direcciones con las que éstas concretaron alguna operación antes o después– fueron publicadas en algún sitio o perfil, como así también si se encuentran asociadas a una casa de cambio virtual o *"exchanges"*, a plataformas de "billeteras virtuales" o a otra compañía que brinde servicios relacionados con criptoactivos.

Resta mencionar que otro método para alcanzar la "desanonimización" de una dirección determinada consiste en explotar la "trazabilidad" inherente a la mayoría de los criptoactivos.

En efecto, aun cuando no se logre identificar a la persona detrás de una dirección determinada, es posible analizar en la cadena de bloques las operaciones plasmadas antes o después del incidente, hasta dar con una dirección conocida o identificada por alguno de los medios ya mencionados.

Tras ello y en caso de resultar posible, podría requerírsele al administrador de la dirección la información vinculada al pagador, y así sucesivamente hasta llegar a la persona detrás de la dirección de interés para el caso. Cabe señalar que la efectividad de este método de investigación se va a ver afectada por las distintas maniobras que los autores puedan pergeñar para entorpecer la trazabilidad.

7.4. Técnicas de ofuscación

Es posible que el seguimiento o trazabilidad de las direcciones se vea truncado por la utilización de procedimientos conocidos como "coinjoin"[37] o servicios identificados como "mixers" o "tumblers"[38], en los cuales el interesado en obstaculizar la trazabilidad de sus fondos transfiere los mismos a la dirección provista por la plataforma que provee el servicio, encargándose de llevar a cabo múltiples operaciones que tienden a desorientar a quien intente seguir el rastro de las mismas, debido a la cantidad de transacciones, grado de atomización, introducción de fondos en la operatoria provistos por diversos usuarios e incluso, en ciertos casos, al uso del procedimiento "coinjoin".

A su vez, algunos proveedores de estos servicios se jactan de contar con reservas de criptoactivos que ya fueron procesados mediante este sistema, para poder darle así una solución inmediata al usuario, por lo que aun en el remoto caso de poder individualizar al presunto destinatario de los fondos introducidos al sistema, no será posible vincularlo a la maniobra que nos ocupa.

En estos casos, la fisonomía de las transacciones puede brindarnos algunos indicios para evaluar, en un caso concreto, si nos halláramos o no ante alguno de estos[39].

De hecho, la información que sí se plasma en la cadena de bloques de Bitcoin con motivo de su funcionamiento se presenta como una operación similar a cualquier otra, sin mayores particularidades, sin que deje entrever el uso de la red "Lighting Network"[40] y, mucho menos, la numerosa cantidad de operaciones que podrían haber tenido lugar detrás de aquella transacción visible.

7.5. Identificadores o selectores de búsqueda

Partiendo de estas consideraciones, para poder emprender una investigación mediante la explotación de los recursos mencionados anteriormente, es decir, a través del análisis de la información almacenada en la cadena de bloques y diferentes fuentes de información de acceso público, será necesario contar con un identificador válido y, en la medida de lo posible, saber a qué plataforma de criptoactivos corresponde.

Los selectores de búsqueda **más relevantes dentro del ecosistema son las direcciones y los identificadores de las transacciones. En lo que respecta a las primeras, su formato puede variar de**

37. Si bien las operaciones de este tipo revisten cierta complejidad –y por ende, sigue siendo la excepción a la regla–, existen ya diversas billeteras y plataformas que incorporan herramientas basadas en este sistema y lo presentan con una interfaz gráfica y fácil de utilizar –samouraiwallet.com y wasabiwallet.io, entre otras–.

38. Estos son servicios que se utilizan para mezclar los fondos de una dirección con los de otras, a fin de confundir el flujo de las operaciones y hacer que se pierda el rastro las mismas. La mayoría de estos sitios tienen enlaces visibles en la web superficial –https://chipmixer.com/ y https://coinmixer-es.net–, aunque también existen dominios vinculados a la web profunda, lo cual agrega una capa extra de complejidad para llevar adelante nuestras investigaciones.

39. A los efectos de conocer los diferentes recursos de los que se valen estas herramientas y algunas las características apreciables que podrían dar cuenta de su uso, puede accederse al sitio https://en.bitcoin.it/wiki/Privacy.

40. Para mayores detalles sobre su funcionamiento, puede visitarse el sitio http://lightning.network/docs/

una plataforma a otra. Mencionamos anteriormente que las direcciones de Bitcoin se caracterizan por tratarse de una sucesión de caracteres alfanuméricos que comienzan con el número "1", el número "3" o con los caracteres "bc1q" o "bc1p", y que poseen una extensión de entre 26 y 35 caracteres, para los primeros dos supuestos, y de hasta 90 caracteres para los dos restantes.

Por otro lado, en la red Ethereum las direcciones se expresan con caracteres alfanuméricos también, puntualmente, hexadecimales[41], y su extensión asciende a cuarenta y dos dígitos, entre los que se incluye el prefijo "0x"[42]. Este formato de direcciones resultará válido tanto para el criptoactivo Ether como para todos aquéllos que funcionen como "tokens" sobre la red Ethereum.

Existe un amplio espectro de plataformas y, por ende, formatos de direcciones. De hecho, si bien Ethereum es una de las redes más conocidas sobre la que funcionan una multiplicad de "tokens", existe un gran número de plataformas que admiten este tipo de implementaciones.

Del mismo modo, es posible que un activo funcione sobre múltiples plataformas, tal es el caso de algunos activos estables de gran circulación, como por ejemplo Tether, cuyas unidades pueden ser emitidas y transferidas sobre Ethereum, pero también sobre las plataformas denominadas EOS, Tron y Algorand, entre otras. Es decir que podremos encontrarnos con direcciones de aquéllos criptoactivos en formatos variados.

Algunas plataformas de análisis brindan sus servicios con relación a múltiples criptoactivos y cuentan, a su vez, con buscadores que detectan de forma automática a cuál o cuáles de ellas podría pertenecer una dirección determinada, lo que podría ser de utilidad para establecer tal extremo, entre las mismas se encuentran:

- **Blockchair** (https://blockchair.com/)
- **Blockcypher** (https://live.blockcypher.com/)
- **Blockchain.com** (https://www.blockchain.com/)
- **BTC.com** (https://btc.com/).

El identificador de las transacciones ("identificador *hash*", *"Hash ID"* o "TXID"), como señalamos anteriormente, es un valor que se obtiene mediante la aplicación de funciones hash sobre los datos de la operación en cuestión. En este caso, será de vital importancia conocer a qué plataforma de

41. En rigor, se expresan en sistema hexadecimal, lo que quiere decir que cada dígito estará representado por un número del "0" al "9" o alguna de las letras comprendidas entre la "a" y la "f".

42. Cabe señalar que dicho prefijo suele encontrarse en todo número o dato expresado en sistema hexadecimal, por lo que no constituye una particularidad exclusiva de las direcciones de Ethereum.

criptoactivos corresponde el identificador en cuestión, ya que su formato se replica en un gran número de implementaciones.

Ahora bien, al ser el resultado de funciones hash, es virtualmente imposible que el valor resultante se replique en diferentes plataformas[43], por lo que podría intentarse una consulta por medio de buscadores que analicen distintas redes y, en caso de dar con un resultado positivo en alguna de ellas, estaríamos en condiciones de afirmar que probablemente nos hallemos ante la transacción de interés para el caso.

7.6. Análisis de transacciones

Una vez que contemos con una dirección o una transacción correctamente individualizada en su respectiva cadena de bloques, podemos avanzar con el análisis. Las plataformas mencionadas anteriormente podrán ser de utilidad en la mayoría de los casos, mientras que, para otros activos, será necesario realizar algunas averiguaciones para dar con una plataforma que visibilice el contenido de su respectiva base de datos.

Para el caso específico de Bitcoin, se podrán utilizar las plataformas mencionadas anteriormente, aunque también otras desarrolladas específicamente para dicha red, como por ejemplo OXT (https://oxt.me/) y WalletExplorer (https://www.walletexplorer.com/), mientras que, para la red Ethereum, es posible recurrir a Etherscan (https://etherscan.io/).

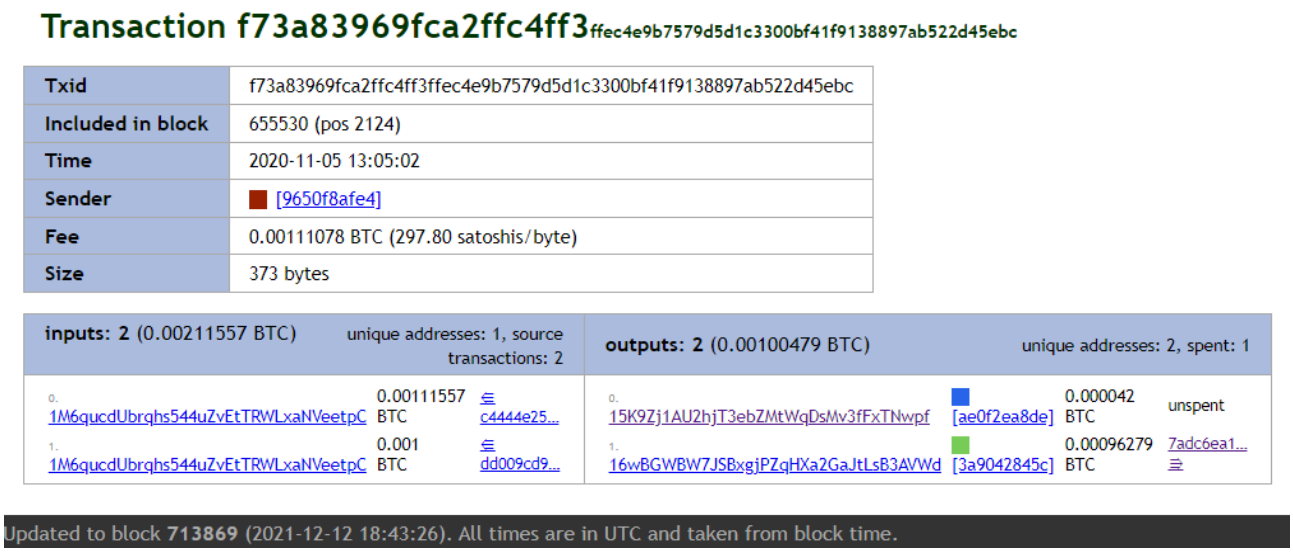
Adicionalmente, para búsquedas en la red BNB Chain, puede utilizarse el explorador BSC Scan (https://bscscan.com/). Si bien no ocupa el lugar de las dos principales "blockchain" del ecosistema – Bitcoin y Ethereum- BNB Chain ha ganado relevancia a lo largo de los últimos años por la incipiente y exponencial creación de tokens relacionados a negocios de "finanzas descentralizadas" que funcionan sobre la base de contratos inteligentes con costos reducidos (los "fees" o costos de transacción de la red se caracterizan por ser sustancialmente más bajos que los de sus principales competidores). Son éstas las características que han vuelto a BNB Chain una red comúnmente utilizada para el despliegue de sistemas engañosos o fraudulentos, por lo que las búsquedas en esta "blockchain" deben siempre tenerse en cuenta como parte del proceso de una investigación orientada a conductas delictivas con criptoactivos.

Otra plataforma que admite contratos inteligentes y presenta también una amplia adopción -por motivos similares- es Tron. Para su análisis, se sugiere utilizar el explorador Tronscan (https://tronscan.org/).

43. Como excepción a esta afirmación, debemos tener en cuenta que algunas cadenas de bloques no surgen desde cero, es decir, de una base de datos en blanco, sino que nacen, por motivos de variada naturaleza, como las bifurcaciones de bases de datos preexistentes. Tal es el caso de Ethereum y Ethereum classic, por ejemplo, o Bitcoin y Bitcoin cash. En estos supuestos, las transacciones registradas con anterioridad a la bifurcación coexistirán en ambas bases de datos. Y lo mismo sucederá con aquellas direcciones utilizadas en la red originaria con anterioridad a la bifurcación, aunque, luego de esto, las operaciones que en las que sean usadas serán consignadas en la cadena de bloques de la red en la que se comunique la transacción.

7.6.1) Búsquedas mediante Identificador de la transacción (TXID)

Al realizar la búsqueda a partir del identificador de una transacción, la plataforma arrojará un resultado similar al que se exhibe a continuación:



Transaction f73a83969fca2ffc4ff3ffec4e9b7579d5d1c3300bf41f9138897ab522d45ebc

Txid	f73a83969fca2ffc4ff3ffec4e9b7579d5d1c3300bf41f9138897ab522d45ebc
Included in block	655530 (pos 2124)
Time	2020-11-05 13:05:02
Sender	[9650f8afe4]
Fee	0.00111078 BTC (297.80 satoshis/byte)
Size	373 bytes

inputs: 2 (0.00211557 BTC)	unique addresses: 1, source transactions: 2		**outputs: 2** (0.00100479 BTC)	unique addresses: 2, spent: 1	
0. 1M6qucdUbrqhs544uZvEtTRWLxaNVeetpC	0.00111557 BTC	c4444e25...	0. 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf [ae0f2ea8de]	0.000042 BTC	unspent
1. 1M6qucdUbrqhs544uZvEtTRWLxaNVeetpC	0.001 BTC	dd009cd9...	1. 16wBGWBW7JSBxgjPZqHXa2GaJtLsB3AVWd [3a9042845c]	0.00096279 BTC	7adc6ea1...

Updated to block **713869** (2021-12-12 18:43:26). All times are in UTC and taken from block time.

El ejemplo ilustrado corresponde a una operación realizada sobre la red Bitcoin[44], sin embargo, nos encontraremos con los mismos campos de información al realizar el análisis sobre otras redes.

Además del "hash" correspondiente al identificador de la transacción –"TxID"–, se observa un campo en el que se indica el número del bloque y la posición, dentro de aquél, en la que la operación fue incorporada –"Included in block"–. El tiempo consignado –"time"– es el horario en el que la transacción fue generada por el usuario que envió lo fondos, debe prestarse atención al huso horario utilizado por la plataforma –en este caso, UTC–. Se incluye también la comisión asignada en la operación para el minero –"Fee"– que será, en definitiva, el resultado de restarle a la cantidad de criptoactivos enviados el valor recibido por las direcciones de destino. Finalmente, se puede observar el tamaño de la operación –"size"–, es decir, el espacio de memoria que ocupan las líneas de código que la conforman.

La plataforma ilustra, además, en uno de sus campos, el identificador de la "billetera" desde la que los fondos fueron enviados –"Sender"–, sin embargo, se trata de un valor generado por la propia plataforma de análisis, sobre el que volveremos luego, pero que no constituye, en definitiva, un identificador propio de este tipo de activos.

44. El ejemplo propuesto fue tomado de https://www.walletexplorer.com/.

Luego nos encontramos con los campos de entrada y salida –"Inputs" y "Outputs"–. En estos se consignan las direcciones de origen y las de destino de la transacción, consignándose además, en cada caso, la cantidad de activos enviados y recibidos por cada una de las direcciones involucradas.

Es posible que nos encontremos con direcciones repetidas en ambos campos. Como se explicó anteriormente, con cada operación que se realiza en la red Bitcoin, quien envía activos debe superar una prueba consignada en la operación precedente. Cuando un usuario recibe activos provenientes de múltiples operaciones en una única dirección, para disponer de todos sus valores, deberá generar una operación que involucre la realización del proceso de validación por cada una de las operaciones de origen, lo que traerá aparejado que, al observar la transacción, se presente en el campo de origen una misma dirección en múltiples ocasiones.

A su vez, como señalamos anteriormente, el envío de activos debe involucrar la totalidad de los valores asignados a una dirección, aun cuando el emisor necesite transferirle a un tercero únicamente un porcentaje de los fondos. En estos casos, quien realiza la transacción puede enviar el porcentaje correspondiente a la dirección de aquél tercero y, el monto restante, a una dirección controlada por él, pudiendo ser la misma que utilizó para el envío o, como se aconseja dentro del ecosistema, una "dirección de cambio", es decir una dirección que no ha sido utilizada, y que se genera en la ocasión para recibir aquellos activos virtuales.

Esta particularidad no se da en otros casos. Sin ir más lejos, en la red Ethereum es posible realizar transferencias parciales, y las direcciones suelen ser reutilizadas por sus usuarios.

7.6.2) Búsqueda mediante direcciones

Si el punto de partida para la investigación es una dirección, al consignarla en una plataforma de análisis, podremos observar un detalle de la totalidad de las transacciones en las que se haya visto involucrada:

Address 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf

part of wallet [ae0f2ea8de]

Page 1 / 1 (total transactions: 23)

date	received/sent	balance	transaction
2020-11-05 13:31:21	+0.000063	0.00090748	7adc6ea16065560d2bb89c1f1dd8b04847ecd5c145af3b63173a26a89241b22b
2020-11-05 13:05:02	+0.000042	0.00084448	f73a83969fca2ffc4ff3ffec4e9b7579d5d1c3300bf41f9138897ab522d45ebc
2020-10-28 05:59:48	+0.00001	0.00080248	504ee1adf4c22111b5f3cf4ce3b27a3d9b305e67ad6c431fce7eba9614ebc56e
2020-10-28 05:59:48	+0.00006	0.00079248	3f1c7e1c124fa9c6dabe16a378bf7380d30ad3fa663735224b51c496549bda22
2020-10-28 05:12:11	+0.00005	0.00073248	c70acd351ac25c485635d9a34a718f1d486e830aacd2f5380f4c412c9c85ce86
2020-10-26 06:47:57	+0.00002	0.00068248	34bace085df56c95bbd6e470bf05228b19faeafc0e4f8838db46d6000eebceb4
2020-10-26 05:55:30	+0.000032	0.00066248	8028b376f3970457f018749890298b9d8e758311d16a3f94d740c44b89924b7d
2020-10-26 05:41:01	+0.0000555	0.00063048	4c5f9d70a69b941ca5470907c700b4b104ce04782f038ba70e082eec9a05114d
2020-10-26 05:29:13	+0.00004	0.00057498	de277b962d1f4f26ff1a7e5445710803e91f8b79f37516bda988de53da832bb2
2020-10-25 14:57:38	+0.000042	0.00053498	af2fa766741d852daf9b52acc84fdb29939b4760c828fb81e4e0b397bd411252
2020-10-19 03:43:39	+0.00024657	0.00049298	d34fcdbf2d67ae8836553a624b1e562a0e0816e4c82faa4e44f6d56e1228fbc0
2020-10-19 03:43:39	+0.00008597	0.00024641	44f4c170d00f13b589e5bf8412c7bd35307560f13bf3daf6e63fad5812124ff2
2020-10-16 22:59:20	+0.00008797	0.00016044	159cdf02292b0621bc18618b66cf9c63e60e809dec89b44ff4e3006632635999
2020-10-16 10:56:24	+0.00002832	0.00007247	ebf85ffa51daf7e7fbe2a9ac75fdfc9c4b1d381dd406a108f8e6761ab749d12c
2020-10-16 10:46:30	+0.00004415	0.00004415	12e811503852dfc661a24d716dbacd72e379499ee6cc256f0e00b76127fa0982
2018-10-28 17:08:36	-0.00594775	0.	87b2309f38e69b89867ea99e6dd77c691fb3a687343e280ebf26df53689aa200
2018-03-27 14:06:10	+0.00594775	0.00594775	cdfddcdc71b22e20054da0541f622d8b1535305ee616669d02d5ba29479d9abd
2018-02-05 16:35:43	-0.006	0.	c1a273b2401ca4723ccf386207d073fd7f450cecbb9a38c3f299a3f2ff3333c3
2018-01-22 00:05:49	+0.006	0.006	38cbae478ee96f0d701f8f118218fc953b7e940e3444d195bea030181a472276
2017-12-01 19:55:33	-0.07574079	0.	a712f4c97af83898ca551e58d184fe4a567f340c106af9b89e98f7500c8383b2
2017-11-30 14:01:05	+0.07574079	0.07574079	07910d31255e3fad18a9128c7ffcfcacb4aa038d0cd911da122853e864c0e745
2017-11-13 00:34:18	-0.00176741	0.	b535babca3ce9945e50426674cafe9436f4de8605daeb4edd288b5571363ce8c
2017-11-01 15:33:23	+0.00176741	0.00176741	627d5a8d0e195f4c77a37f629cdee7256d208f8ff904236e4b42815b405dfe2b

Page 1 / 1 (total transactions: 23)

Updated to block **713869** (2021-12-12 18:43:26). All times are in UTC and taken from block time.

Si bien las distintas plataformas presentan la información con diferentes formatos, todas ellas exhibirán mínimamente la fecha y hora de cada una de las operaciones, el identificador de la transacción y los montos transferidos. Un primer examen nos permitirá evaluar aspectos vinculados a la actividad del usuario detrás de la dirección, concretamente, el volumen de activos y transacciones que realiza, y los horarios en los que opera[45].

45. Para un análisis de los días y horarios de actividad de las direcciones, se sugiere recurrir a la plataforma OXT (https://oxt.me/) que, entre otras funcionalidades, ofrece gráficos que ilustran estos aspectos.

7.6.3) Utilización del agrupado y etiquetado

Ahora bien, si el objetivo de la labor se centra en la individualización de la persona detrás de una dirección, el "agrupado" y el análisis de las operaciones partiendo de las entidades adquiere suma relevancia, teniendo en cuenta las particularidades de aquellas **técnicas que mencionamos anteriormente, y que permiten extender el catálogo de direcciones etiquetadas, lo que aumenta las probabilidades de encontrarnos con una de ellas al realizar el análisis correspondiente.**

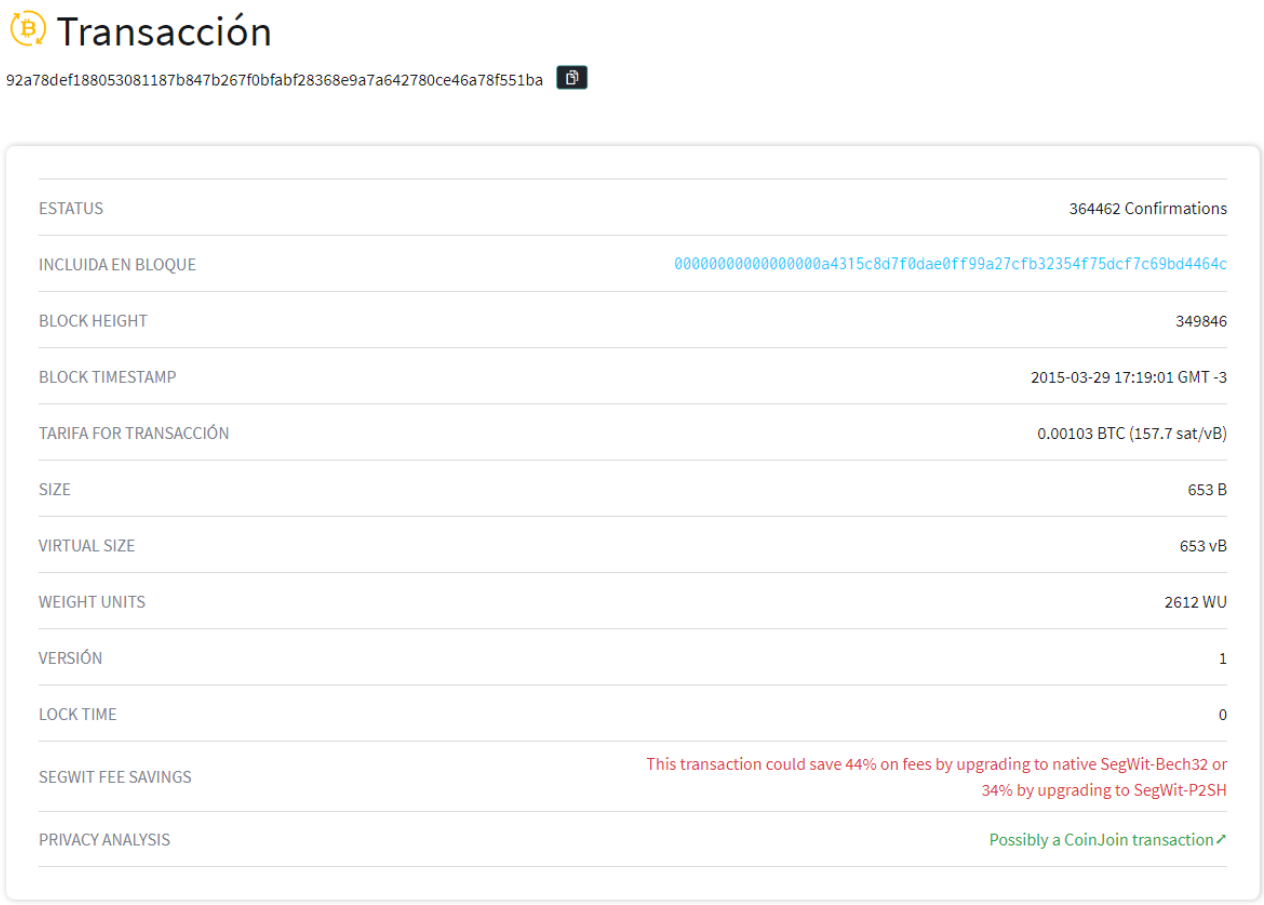
Puede recurrirse, para este tipo de análisis, a algunas plataformas gratuitas que se valen de las referidas técnicas de "agrupado" y "etiquetado". Entre éstas, nos encontramos con las ya mencionadas WalletExplorer y OXT, específicamente para Bitcoin, y Etherscan.io para la red Ethereum. A su vez, cabe mencionar otros sitios web como https://bitcoinwhoswho.com/, https://www.bitcoinabuse.com/ y https://checkbitcoinaddress.com/ que, si bien no se valen de técnicas de agrupado, recolectan y aportan cierta información que podría resultar de interés para este tipo de casos.

Es posible emprender una labor tendiente a identificar a la persona que controla cierta dirección realizando consultas en las plataformas mencionadas, sin embargo, sería poco probable que la dirección utilizada por los autores de una maniobra bajo investigación se encuentre "etiquetada" en alguna base de datos. Claro que las probabilidades aumentan en la medida que avanzamos sobre las sucesivas transacciones vinculadas.

La premisa de la que suele partirse al realizar este tipo de investigaciones consiste en que los fondos habidos en una dirección serán consumidos oportunamente, total o parcialmente, es decir que serán transferidos a una o más direcciones, y a partir de alguna de esas nuevas direcciones podría encontrase asociada a una entidad "etiquetada".

Dicho proceso, como se comentó anteriormente, puede repetirse indefinidamente hasta dar con una dirección "etiquetada", siendo el principal obstáculo con el que podemos encontrarnos el volumen de información a analizar, en función de la cantidad de ramificaciones que pueden generarse con cada transacción sobre la que avancemos y, en segundo lugar, el uso de alguno de los diferentes sistemas que obstaculizan en diferente medida la trazabilidad.

Se sugiere, para el caso de encontrarnos con operaciones atípicas –por ejemplo, transacciones que involucren numerosas direcciones de origen y de destino simultáneamente–, consultarlas por medio de la plataforma Blockcypher que incluye, entre sus funcionalidades, la detección automática de indicios que puedan dar cuenta del posible uso de recursos derivados de la técnica de "coinjoin":



Adicionalmente, debe considerarse que para lograr la identificación y el "etiquetado" de potenciales transacciones en las que se haya utilizado la técnica "coinjoin", estos sistemas se basan en un conjunto de parámetros y criterios generales de sospecha que pueden ser extraídos y aplicados a un procedimiento de investigación. De esta forma, independientemente de la utilización o no de un software específico, se sugiere que a la hora de efectuar maniobras de exploración de transacciones en una "blockchain" se tenga siempre en consideración algunos criterios básicos. Estos, aplicados a un caso concreto, pueden resultar de utilidad para la detección "humana" de operaciones de índole sospechoso o relevantes para la investigación, potencialmente fruto de maniobras de "coinjoin" o "mixing" de transacciones[46], entre otras, por ejemplo:

- Existencia de transacciones donde el número de direcciones de origen, desde donde parten los fondos, es significativamente inferior al número de dirección/es de destino.

46. Estos criterios pueden extraerse del trabajo de investigación realizado por la School of Mathematical & Computer Sciences de la Universidad de Heriot Watt (Edinburgo, Escocia), publicado en abril del 2022 (https://researchportal.hw.ac.uk/en/publications/the-unique-dressing-of-transactions-wasabi-coinjoin-transaction-d). Cabe destacar que el método utilizado en dicho trabajo se orientó a extraer específicamente criterios que permitieran detectar la utilización de un sistema de "coinjoin" específico, no obstante, las conclusiones de índole general a las que se arriba resultan útiles como "señales de alerta" o "criterios de investigación" para casos que involucren la utilización de cualquier sistema o software de este tipo.

- Existencia de un patrón de transacciones concomitantes con lo descripto en el punto anterior, que –con independencia de la similitud o no de las direcciones de origen- coincidan en su/s dirección/es de destino.

- Coincidencia en el tipo de direcciones de origen, en especial si se utilizan direcciones del tipo "Segwit" o "Taproot" usualmente aplicadas para este tipo de maniobras.

7.6.4) Solicitudes de registros de usuario

Si la investigación nos permite arribar, tras una serie de pasos, a una dirección "etiquetada", dependiendo del tipo de empresa o plataforma señalada, y teniendo en cuenta las normas y las políticas de la empresa en lo que respecta al suministro de información de sus clientes, podremos requerirle ciertos datos que nos podrían permitir individualizar, cuanto menos, a la persona detrás de aquélla última operación de la cadena de transacciones relevadas.

Una porción considerable de las direcciones "etiquetadas" suele pertenecer a plataformas dedicadas al intercambio de activos ("Exchanges"), o que ofrecen servicios o productos a la venta y aceptan pagos con criptoactivos, es decir, plataformas con las que los usuarios de criptoactivos suelen operar para obtener un provecho en una especie diferente, ya sea dinero fiduciario, bienes o servicios de diferente naturaleza.

Algunas de estas empresas intentan adecuar sus políticas a las normas y recomendaciones antilavado[47], y en línea con ello, adoptan procedimientos tendientes a verificar la identidad de sus clientes. Como se refirió anteriormente estas buenas prácticas parten de modelos de autoregulación, pues si adicionalmente no prestan servicios financieros o de crédito o alguna otra actividad designada por la ley de prevención del lavado de dinero, estas empresas no están alcanzadas expresamente por las obligaciones y regulaciones que impone la ley a los sujetos obligados. A su vez, pueden contar en ocasiones con información relativa a cuentas bancarias, tarjetas de crédito y otros medios de pago asociados por el usuario a su cuenta. También contarán con información relativa a su registro, como direcciones de correo electrónico y números de teléfono, y detalles de sus accesos a las cuentas, es decir, las direcciones IP.

Claro que, además de ello, contarán con un detalle de las transacciones realizadas, por lo que en caso de requerirle información sobre el usuario que podría haber recibido o enviado fondos, en el marco de una transacción que tuvo como destino una dirección que podría pertenecer a dicha plataforma, debería bastar con suministrarle la información relativa a la transacción en cuestión –fecha, hora, identificador de la transacción, direcciones de origen, direcciones de destino, montos transferidos–,

47. Al respecto, cabe mencionar que en mayo de 2022 el Poder Ejecutivo Nacional presentó ante el Congreso un proyecto de reforma de la Ley N° 25.246 que, entre otras modificaciones relativas al sistema de PLA/CFT, prevé la incorporación de los PSAV como sujetos obligados. https://www.argentina.gob.ar/noticias/despues-de-once-anos-se-propone-en-argentina-una-reforma-sustancial-del-sistema-placft

para que la empresa pueda identificar al cliente asociado a la misma.

En función de lo que se desprenda de la información provista, como así también, de la distancia entre la operación traída inicialmente a estudio y la transacción que tuvo como destino la dirección "etiquetada", deberá evaluarse su posible vinculación con la maniobra investigada y, dependiendo de ello, si existen elementos para imputarle el hecho. En su defecto, podrá optarse por solicitarle información sobre el negocio que motivó aquella transacción, en aras de continuar identificando a quienes realizaron las sucesivas operaciones hasta arribar a la dirección que, de acuerdo a la teoría del caso, podría ser controlada por los autores o partícipes de la maniobra.

8. POSIBLES EVIDENCIAS FORENSES

Los investigadores forenses reciben capacitación rutinaria para identificar evidencias tradicionales como equipos, dispositivos electrónicos, unidades de almacenamiento, ciertos datos técnicos y otros elementos como por ejemplo notas que pudiesen representar contraseñas. En la actualidad, dicha información resulta vital en un contexto en el que los sospechosos utilizan con mayor frecuencia el cifrado, por tal motivo encontrar una contraseña puede ser muy útil.

En tal sentido, las evidencias vinculadas con el uso de criptoactivos se suman como una nueva categoría de elementos que se deben identificar, tanto en el lugar del hecho como en los laboratorios forenses donde se examinan computadoras, unidades de almacenamiento, teléfonos móviles y tabletas. Si bien estos indicios pueden resultar novedosos, su búsqueda no debería resultar compleja, debido a que, desde hace tiempo los investigadores forenses se han capacitado para identificar contraseñas en notas adhesivas, cuadernos y escritos en hojas de papel.

Un obstáculo adicional a la hora de requerir información de empresas proveedoras de servicios de intercambio o compraventa de criptoactivos a través de internet es que, por la naturaleza y entorno digital de su negocio, esas empresas podrían estar constituídas y operar en jurisdicciones extranjeras, con lo cual el acceso a este tipo de información y evidencia digital puede resultar más complicado[48].

8.1. Documentos escritos e impresos

En tal caso, las contraseñas son bastante fáciles de identificar porque son una simple palabra o frase escrita, a menudo sin contexto. Sería incluso mejor obtener una contraseña compleja con números y caracteres, que a menudo será claramente identificable como tal. De forma análoga, encontrar evidencia del uso de criptoactivos podría resultar igual de sencillo una vez que nos encontramos familiarizados con esta tecnología.

8.1.1) Direcciones públicas

Como ya mencionamos anteriormente, las direcciones de Bitcoin comienzan con el número 1, el número 3 o con los caracteres “bc1”, los dos primeros formatos poseen una extensión de entre 26 y 35 caracteres, y una longitud de hasta 90 caracteres para el restante. Por ejemplo:

- 1Lz7EXCqydMVkb5twX7kr8Y4N4PZzAuLPK (Base58)

48. Sugerimos recurrir, para mayor información, a la “Guía de buenas prácticas para obtener evidencia electrónica en el extranjero” (https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf) y a la “Guía de obtención, preservación y tratamiento de evidencia digital” (https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf).

- 3M3imw63BUiUEpNvJHcSd6CHRD4dHJxEnL (Base58)
- bc1q270ahlz47xchvw02a9r44mdu9v6tfx0589043v (Bench32)

Por otro lado, las direcciones de Ethereum comienzan con 0x y tienen 42 caracteres.

- 0x66febdddc377e2ee0b997c72b76d12c4aa2ce9be

Estos ejemplos permiten facilitar la identificación de este tipo de indicios a simple vista, principalmente porque debería resultar llamativo encontrarse con documentos donde se encuentren plasmados una serie de caracteres aparentemente aleatorios, que claramente no es un número de teléfono o un número de cuenta bancaria, sino algo que más bien se asemeja a una contraseña muy peculiar. Algunos de los lugares donde podrían llegar a encontrar son:

- Anotaciones en pizarras.
- Correo electrónico impreso
- Impresiones en papel de un archivo.
- Notas adhesivas.
- Tarjetas de presentación.
- Códigos QR.

8.1.2) Claves privadas

Estas se pueden encontrar en tarjetas de regalo preimpresas u otras billeteras de papel como las mencionadas en el presente documento. Debemos recordar que, si una billetera en papel contiene la clave privada, esto le permite al poseedor tomar el control de los fondos, situación que sería de interés al momento de realizar la incautación de su contenido.

Aunque es posible que los usuarios no protejan tanto la clave pública, tienden a ser más cuidadosos cuando se trata de la clave privada. Es poco probable que las claves privadas se escriban en una hoja de papel y se desechen, pero se pueden encontrar resguardadas en cajones, libros, archivadores o cajas fuertes.

Las claves privadas de Bitcoin pueden estar en varios formatos y se recomienda fuertemente que los investigadores las reconozcan. Existen claves alfanuméricas que tienen los siguientes formatos:

- Claves de formato hexadecimal estándar de 256 bits y 64 caracteres de largo

- Claves en formato de importación de billetera (WIF), estas poseen una longitud de 51 caracteres y comienzan con el número 5.

- Claves de formato mini privado, en estos casos la cadena tiene 21 caracteres de longitud.

Asimismo, resulta oportuno señalar que las claves privadas de Ethereum tienen 64 caracteres. Por ejemplo: aba7e63318ebe4450911b62d5e79139310ad35545338bb89fcb7183365cc3375.

Por otro lado, como ya se mencionó, las claves privadas también pueden tener la forma de una cadena de palabras de código mnemotécnico o "semilla", situación que debería llamar la atención del investigador por tratarse de una lista de palabras escritas a mano o mecanografiadas que no se relacionan entre sí.

Todos estos elementos son bastante fáciles de reconocer y asimilar, facilitando que los investigadores forenses los reconozcan sin necesidad de contar con información técnica detallada, asegurando mediante su preservación que no se pierda información potencialmente vital.

8.2. Dispositivos electrónicos

Podría decirse que dispositivos electrónicos tales como computadoras, unidades de almacenamiento, teléfonos móviles y tabletas, se incautan prácticamente de forma rutinaria durante el curso de casi cualquier tipo de investigación. Incluso solo un pequeño porcentaje de las investigaciones digitales son en realidad delitos informáticos y prácticamente en cualquier delito puede encontrase asociada evidencia digital.

Por otro lado, debido a la masificación del uso de criptoactivos, los delitos vinculados en algún aspecto con esta tecnología resultan y resultarán mucho más frecuentes, situación que nos lleva a replantear ciertos interrogantes en este tipo de escenarios investigativos mediante la adaptación de técnicas forenses que se practican habitualmente en la búsqueda de determinadas evidencias forenses.

8.2.1) Programas o aplicaciones instaladas

Para el caso de estos dispositivos, independientemente del modelo y sistemas operativos, se recomienda verificar la existencia de billeteras de software, no solamente instaladas en los mismos sino también aquellas versiones portátiles que pueden ejecutarse sin necesidad de instalación previa.

Cada uno de estos programas y aplicaciones gestiona de manera diferente el almacenamiento y

tipo de registros informáticos que resguardan, los que podrían resultar de interés para nuestras investigaciones[49].

Por otro lado, es recomendable verificar la existencia de programas o aplicaciones utilizadas para gestionar contraseñas, debido a que podrían contener registros vinculados al conjunto de claves pública/privada en sus diferentes formatos y/o cadenas de palabras de código mnemotécnico o "semillas".

8.2.2) Historial de Internet

En este caso resulta altamente recomendable verificar el historial de navegación web disponible a partir de los registros almacenados en los dispositivos, a fin de corroborar el acceso a sitios vinculados con la generación de billeteras frías o incluso plataformas de intercambio de criptoactivos.

8.2.3) Correos electrónicos y servicios de mensajería

Mediante el análisis de estos elementos resultaría posible identificar conversaciones vinculadas con el uso de criptoactivos, como por ejemplo intercambio de direcciones y comprobantes de transferencias.

8.2.4) **Documentos de ofimática** e imágenes

Es posible que estos registros expongan información correspondiente al conjunto de claves pública/privada en sus diferentes formatos, cadenas de palabras de código mnemotécnico o "semillas", como así también información codificada en formato QR.

49. En este aspecto resulta oportuno mencionar la existencia de ciertos registros informáticos que una vez identificados podrían aportar información vinculada con el conjunto de claves público/privada, transacciones enviadas y recibidas, identificador de las transacciones, etc. A modo de ejemplo se pueden citar los archivos "wallet.dat" de Bitcoin Core y "wallet.log" de Bitcoin Wallet.

9. INCAUTACIÓN DE CRIPTOACTIVOS

En la actualidad existe un debate abierto sobre los procedimientos correctos para la incautación de criptoactivos, ya sea durante el desarrollo de una investigación, en la escena del crimen en vivo o de forma posterior en los laboratorios forenses, por tal motivo en este documento se presentan una serie de recomendaciones que no deben interpretarse como la única forma de proceder, menos aún en este complejo y dinámico entorno digital[50].

En caso de que se tenga la sospecha -a partir del análisis de la información del caso- de que en el marco de un operativo podría surgir la posibilidad de incautar criptoactivos, constituye una buena práctica adoptar previamente los recaudos necesarios para que la fuerza designada cuente con los elementos suficientes para poder avanzar en ese sentido.

Del mismo modo, deberían tramitarse las autorizaciones necesarias para llevar a cabo la incautación de los activos por medio del procedimiento por el que se vaya a optar en el caso concreto. En este sentido, cabe reparar en que la facultad de ordenar el secuestro y la custodia de los efectos secuestrados corresponde al Juez del caso, de acuerdo a lo establecido en Código Procesal Penal de la Nación (arts. 231 y 233),

Por otro lado, resulta más que oportuno destacar la importancia de realizar estas medidas en tiempo y oportunidad, debido a que, para el caso de los criptoactivos, quién tenga acceso a las claves privadas podrá gestionar sus valores de forma remota, aun cuando fueran secuestrados los dispositivos electrónicos vinculados a esas direcciones.

Nos referimos en el presente capítulo a aquellos procedimientos de incautación que no pueden ser llevados a cabo a través de la mera orden dirigida a un tercero. En efecto, cuando los activos se encuentran resguardados en plataformas de arbitraje e intercambio de criptoactivos bastará con librar una orden a la empresa que administra la plataforma en cuestión ordenándole que le aplique, a los valores asociados a la cuenta de los sujetos investigados, el destino que se estime corresponder. De avanzar sobre la incautación, la empresa podrá poner los criptoactivos a disposición mediante su asignación a una cuenta creada dentro de la plataforma a nombre de las autoridades o, eventualmente, mediante su transferencia a direcciones provistas por éstas. Para este último supuesto, podrán tenerse en consideración algunas de las recomendaciones formuladas a continuación.

50. Al respecto, puede ser útil consultar la guía confeccionada por INTERPOL en marzo de 2021 “Guía destinada a los equipos de primera intervención en análisis forense digital”, o bien, la realizada en el marco de GAFILAT en diciembre de 2021 “Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, identificación, Incautación y Decomiso de Activos Virtuales”.

9.1. Consideraciones previas

A diferencia de las monedas convencionales, donde el dinero puede incautarse y depositarse de forma segura por intermedio del sistema bancario tradicional, para el caso de secuestro de criptoactivos, una vez decomisados permanecerán inmutables en la cadena de bloques protegidos por una clave, o un conjunto de claves privadas o "semillas". Dichas claves deben ser resguardadas con la máxima seguridad posible, debido a que si un tercero conociera alguna de ellas podría obtener acceso a los activos incautados.

Más allá de esto, debe tenerse en cuenta que, aunque es posible resguardar los activos en su especie, también se cuenta con la posibilidad de cambiarlos por dinero fiduciario.

El procedimiento podría enmarcarse en el instituto de la venta anticipada, previsto en el art. 3 inc. "f" de la Ley 20.785, debiendo en tal caso ser dispuesto por el tribunal interviniente.

Esta alternativa puede ser útil para evitar la exposición de los bienes a las fluctuaciones y la volatilidad que caracterizan a los criptoactivos y que, en ocasiones, podrían derivar en pérdidas de valor considerables. Claro que estas variaciones en el precio pueden traducirse, también, en una revalorización de los activos. También podría optarse por tal proceder en miras de reducir los eventuales riesgos de seguridad derivados del mantenimiento de los activos y los costos asociados a ello[51].

En definitiva, se sugiere analizar en el caso concreto la conveniencia y la procedencia de una u otra alternativa.

9.2. Pasos para realizar la incautación

En aquellos casos donde se haya decidido proceder a la incautación de criptoactivos, el procedimiento no reviste mayor complejidad que una transacción tradicional utilizando diferentes elementos que ya hemos descripto a lo largo del presente documento.

Sin perjuicio de lo expresado, la operación debe concretarse con sumo cuidado. Buenas prácticas recomiendan concretar las operaciones en pareja, donde uno de los operadores ejecutará las actividades bajo supervisión de su compañero, garantizando la efectividad del procedimiento, siguiendo cada paso de forma cautelosa a fin de reducir riesgos.

51. Tal como se plantea en la ya mencionada "Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, identificación, Incautación y Decomiso de Activos Virtuales" publicada por GAFILAT en diciembre de 2021.

9.2.1) Seleccionar una aplicación para la billetera de destino

En primer lugar, se debe seleccionar el tipo de billetera que será utilizada para recibir la transacción correspondiente a los criptoactivos incautados. Si bien existen varias opciones[52] y tipos de criptoactivos (Bitcoin, Ethereum, etc.), debería tenerse en cuenta el uso de billeteras de software que permitan configurar, en la medida de lo posible, direcciones de firma múltiple con acceso protegido por cifrado.

De esa manera, cuando los fondos se transfieren desde la dirección del sospechoso a una dirección de firma múltiple con dos o más signatarios, no se podrá disponer de estos sin la "autorización" de los otros titulares de claves de la dirección. Esto, sumado a la contraseña de acceso, brinda una capa extra de protección ante la eventual pérdida y/o robo de una de las claves privadas utilizadas para realizar el procedimiento de incautación.

Ahora bien, como ya se mencionó, en la actualidad coexisten miles de criptoactivos diferentes, cada uno de ellos con alguna particularidad que lo distingue del resto. Si bien los programas que funcionan como billeteras virtuales suelen diseñarse para el uso de una amplia variedad de criptoactivos, no se desarrollan con la capacidad de abarcar la totalidad del universo.

En virtud de ello, a la hora de diseñar un plan de acción para la incautación y la eventual restitución de los fondos, se hace necesario evaluar con qué clase de criptoactivos trabajaremos e identificar aquellos servicios o desarrollos que nos permitan trabajar con cada uno ellos. Si bien se reconoce la conveniencia de recurrir a una única solución que permita trabajar con la totalidad de los activos, es posible encontrarse ante casos que requieran del uso de más de una herramienta o plataforma.

9.2.2) Creación de la billetera

Una vez seleccionada la aplicación que se utilizará para recibir los fondos incautados, se deberá proceder a la creación de una billetera a partir de una frase semilla, y resguardar dicha información en un lugar seguro. Luego, será necesario generar las direcciones para cada una de las plataformas sobre las que funcionen los criptoactivos que se pretenden incautar.

Cumplidos estos pasos, no será necesario que la billetera generada a partir de la frase semilla se mantenga en funcionamiento en el dispositivo utilizado, por lo que podrá procederse a eliminar el programa informático y la información asociada al mismo.

En efecto, el uso de este tipo de sistemas no implica en modo alguno que los activos vayan a permanecer resguardados en el dispositivo en el que se instalan. Por el contrario, las operaciones son

52. La selección de una billetera se encuentra vinculada con una serie de factores, como por ejemplo el tipo de dispositivo y sistema operativo que se utilizará para su administración, como así también características de seguridad y privacidad. Para escoger la billetera virtual que mejor se ajuste a nuestras necesidades, se puede consultar el sitio https://bitcoin.org/es/elige-tu-monedero?step=5&platform=windows

almacenadas, como se señaló anteriormente, en la base de datos replicada en múltiples nodos.

De lo expuesto se deduce que es posible recibir criptoactivos en una dirección que se encuentre bajo el control de los investigadores sin necesidad de mantener instalada una aplicación de esta naturaleza.

Bastará con instalar y utilizar uno de estos programas para generar los juegos de claves privadas y públicas; luego las direcciones en las que pretendemos recibir fondos; resguardar la "semilla" en un sitio seguro y, finalmente, eliminar el programa y todos los archivos informáticos asociados a la billetera virtual.

Quien envíe los fondos solo necesitará contar con la dirección de destino, y quien controle esa dirección de destino solo necesitará de una billetera virtual al momento en que desee disponer de los criptoactivos, ocasión en la que podrá instalarla nuevamente e introducir la "semilla" para regenerar las correspondientes claves privadas.

9.2.3) Trasferencia de los fondos

Quizás este paso es el que requiere mayores recaudos, no por presentar una dificultad técnica, sino debido a la correcta verificación que debe realizarse sobre las billeteras de origen y destino a fin de evitar equivocaciones involuntarias que pudieran ocasionar el envío de los fondos incautados a direcciones erróneas.

En tal sentido, existen dos maneras de proceder para realizar la transferencia de fondos que serán incautados, la primera es de "forma directa" mediante la utilización de claves privadas del sospechoso, mientras que la segunda es de "forma indirecta" mediante operaciones realizadas a partir de la propia billetera del mismo.

En el primer caso, de contar con las claves privadas y/o "semillas" del investigado se procederá a importarlas en la billetera de destino, realizando una doble verificación durante el desarrollo del procedimiento entre el operador y el supervisor, comprobando rigurosamente su transcripción y respetando aquellos caracteres que se encuentren en letra mayúscula y minúscula, debido a que las direcciones distinguen esta tipografía.

Una vez verificadas e importadas las claves privadas y/o "semillas", se procederá a constatar su contenido y balance, a fin de realizar el envío y resguardo de la totalidad de criptoactivos en poder del sospechoso hacia la dirección pública creada en el paso anterior.

Por otro lado, de ser posible acceder a los fondos por intermedio de la billetera del sospechoso, se realizará la correspondiente constatación de su contenido y balance, realizando posteriormente el

envío de la totalidad de criptoactivos en poder del sospechoso hacia la dirección pública creada para su resguardo.

9.2.4) Documentación, verificación de la transacción y copias de respaldo

Para finalizar, resultará necesario documentar las actividades realizadas, teniéndose especial consideración en incluir cierta información que será de vital importancia para realizar el posterior análisis de trazabilidad sobre transacciones entrantes y salientes.

En primer lugar y en caso de ser posible, sería oportuno verificar mediante el análisis de la cadena de bloques que el intercambio de criptoactivos se haya realizado con éxito desde la dirección sujeta a medidas cautelares o decomiso hacia la utilizada para su resguardo, realizándose capturas de pantalla, fotografías, consignando en un acta el identificador de la transacción u otro mecanismo para documentar esta actividad.

Por otro lado, en cuanto a los criptoactivos cautelados, será de interés realizar fotografías, capturas de pantalla o documentar de otra manera su origen –direcciones, claves privadas, "semillas", billetera utilizada por el sospechoso–, tipo de criptoactivo y balances.

Respecto de la dirección de destino, deberá resguardarse una copia de seguridad de la billetera de almacenamiento en frío, ya sea en formato papel, mediante su resguardo en un soporte óptico de almacenamiento o ambas, procurando evitar su observación por parte de terceros. La generación de la billetera, la copia de seguridad en formato papel o su almacenamiento en soporte óptico, y su resguardo deberá ser debidamente documentado.

10. ASPECTOS LEGALES

Gran parte de la doctrina coincide en que los criptoactivos son, en cuanto a su naturaleza jurídica, bienes inmateriales[53] y, como tales, pueden integrar el patrimonio de las personas.

Los artículos 15 y 16 del Código Civil y Comercial de la Nación nos indican que las personas son titulares de los derechos individuales sobre los bienes que integran su patrimonio, para luego precisar que aquellos derechos pueden recaer sobre bienes susceptibles de valor económico.

El valor económico de los criptoactivos se presenta con suficiente claridad en la realidad. Los activos de esta naturaleza se comercializan activamente, tanto en nuestro país como en el resto del mundo, a través de diferentes medios y plataformas, a cambio de un precio que, usualmente, se fija en moneda local o extranjera y se determina, fundamentalmente, en función de las reglas de la oferta y la demanda.

Sin embargo, esta clase de activos no gozan de corporeidad. Son parámetros, líneas de código o, en definitiva, conjuntos de bits plasmados en bases de datos que pueden ser procesados e interpretados por medio de dispositivos y programas informáticos. Por tal motivo, son receptados por la categoría subsidiaria del artículo 16 del Código Civil y Comercial de la Nación, que abarca a aquellos bienes que, por su inmaterialidad, no son considerados cosas.

Resta mencionar que, desde una perspectiva técnico-jurídica, los criptoactivos no pueden ser equiparados al concepto de "moneda nacional", en tanto no son emitidos por el Banco Central de la República Argentina (artículo 30 de la Carta Orgánica del Banco Central de la República Argentina, Ley 24.144), y tampoco podrán ser considerados "moneda extranjera", en la medida que no hayan sido emitidos y considerados unidad monetaria por un Estado extranjero.

A pesar de esto, por su carácter de bienes inmateriales, pueden ser objeto de los contratos. De acuerdo a lo previsto en el artículo 764 del Código Civil y Comercial de la Nación, las obligaciones civiles y comerciales pueden incluir, como contraprestación debida, la transmisión o puesta a disposición del acreedor de un bien que no es cosa.

A los fines tributarios, a través del Dictamen N° 2/2022[54], del 16 de junio del 2022, la Administración Federal de Ingresos Públicos (AFIP) se expidió sobre la naturaleza jurídica de las criptomonedas y su tratamiento en el impuesto sobre los bienes personales. Hasta ese momento la AFIP consideraba

53. Tschieder, Vanina Guadalupe en "Derecho & criptoactivos", editorial La Ley, 2020, págs.47 y ss.; Eraso Lomaquiz, Santiago E. en "Las monedas virtuales en el Derecho argentino. Los Bitcoin", revista LaLey, 2015, T. 2016–A, pág. 727; Chomczyk, Andrés en "Regulación de blockchain e identidad digital en América Latina", BID, 2020, pág. 100, accesible en https://publications.iadb.org/es/regulacion-de-blockchain-e-identidad-digital-en-america-latina, entre otros.

54. http://biblioteca.afip.gob.ar/dcp/DID_K_000002_2022_06_16

que las criptomonedas revestían la calidad de "bienes inmateriales", encuadradas en los términos del artículo 19 inciso m) de la Ley N° 23.966 del impuesto sobre los bienes personales y, en consecuencia, les resultaba aplicable la exención prevista en el inciso d) del artículo 21 de la Ley.

Sin embargo, si bien el dictamen 2/2022 no introdujo una modificación expresa a la ley, en este acto que orienta la actuación de sus funcionarios, se modificó el criterio del organismo al entender que las criptomonedas pueden caracterizarse como una nueva clase de activo financiero, no tradicional y basado en la tecnología blockchain, que versa, en definitiva, acerca de una anotación electrónica que incorpora el derecho a una cantidad de dinero determinada.

En esa línea, concluye que las criptomonedas pueden tipificarse como títulos valores, ya que comparten las características principales de estos, es decir, son valores incorporados a un registro de anotaciones en cuenta –la blockchain-, resultan bienes homogéneos y fungibles en los términos del artículo 232 del Código Civil y Comercial, su emisión o agrupación es efectuada en serie –conformada ésta por cada bloque que integra la cadena- y pueden ser susceptibles de tráfico generalizado e impersonal en los mercados financieros.

En definitiva, el Fisco concluyó que las criptomonedas conforman un activo financiero alcanzado por el impuesto sobre los bienes personales, de conformidad con lo prescripto en los artículos 19 inciso j) y 22 inciso h) de la Ley.

Eso tiene una repercusión importante, no sólo por la naturaleza que la AFIP -como organismo público nacional- le otorga a estos activos, sino también porque a partir de este cambio de criterio, estos activos deben ser incluidos en las declaraciones juradas de los contribuyentes, el ente recaudador debería tenerlos identificados, hacer perfiles patrimoniales sobre sus titulares, para confrontar si el origen de los fondos para adquirirlos es coherente con los la información con que cuenta el organismo y, eventualmente, hacer determinaciones de oficio, ejecuciones fiscales, etc.

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO FISCAL | PROCURACIÓN GENERAL DE LA NACIÓN
Av. de Mayo 760 (C1084AAP) - Ciudad Autónoma de Buenos Aires - Argentina
(54-11) 4338-4300
www.mpf.gob.ar | www.fiscales.gob.ar