Bitcoin: herramientas de análisis para abordar investigaciones penales que incluyan operaciones con esta cripto-moneda

Lineamientos para planificar una actividad cautelar eficiente

Sebastián Oppel (*)

Sumario: I. Introducción.— II. Desarrollo.— III. Reflexión final.

I. Introducción

Hablar del Bitcoin **(1)** hoy ya no tiene el impacto de años atrás. Sin dudas su nivel de conocimiento ha aumentado exponencialmente. De una u otra manera, cada vez más gente se ha familiarizado con el término, aunque en la mayoría de los casos no se tenga bien en claro lo que representa o significa, más allá de una aproximación intuitiva en la que se le reconoce valor monetario y se le asigna una entidad completamente digital. Ya sea porque oyeron hablar del Bitcoin en un encuentro familiar, en una noticia periodística difundida por algún medio de comunicación, o bien como consecuencia de la interacción en alguna red social, es probable que cualquier persona dotada de un mínimo grado de conectividad, responda afirmativamente a la pregunta sobre si conoce de su existencia.

En línea con ello, también ha aumentado la cantidad de gente que se ha animado a dar todavía un paso más lejos y se ha introducido en el mundo de esta cripto-moneda —o de alguna otra de las tantas que ha emergido por detrás en el último tiempo— mediante la adquisición de sus unidades de valor, ya sea con fines de inversión desde una óptica especulativa, o bien simplemente como canal de resguardo ante eventuales ciclos inflacionarios que pudieran presentar las monedas fiduciarias, por mencionar tan solo algunos de los tantos posibles motivos. La ola expansiva ha venido acompañada, lógicamente, de la proliferación de una gran cantidad de desarrollos comerciales, tanto a nivel local como internacional, que buscaron acaparar esa demanda, y de la aparición de proyectos innovadores que tuvieron como eje de transformación el uso de la tecnología que respalda al Bitcoin, denominada *blockchain* o "cadena de bloques" **(2)**.

(*) Abogado egresado de la Universidad de Buenos Aires y se desempeña como secretario en el Juzgado Nacional en lo Criminal y Correccional Federal nro. 12. Años atrás cumplió funciones como secretario adjunto en la Unidad Fiscal Especializada en Ciber-delincuencia del MPF. Obtuvo diploma de Especialista por las Universidades de Salamanca y Castilla - La Mancha (Toledo), España, respectivamente.

(1) Siguiendo la terminología empleada por la mayoría de sus desarrolladores actuales (ver https://bitcoin.org/es/vocabulario), utilizaré la palabra "Bitcoin" —con mayúscula— para referirme al protocolo o a la red que lo sustenta; y los términos "bitcoin" o "bitcoins" —sin mayúscula— para referirme a sus unidades de valor.

(2) Definida como un "libro mayor compartido e inmutable que facilita el proceso de registro de transaccio-

Quizá la mejor evidencia de este proceso de 'masificación' —si es que así se puede describir el fenómeno de expansión— lo brindan las modificaciones en materia tributaria que se han introducido en la mayoría de las legislaciones de los países del mundo **(3)**. Bajo diferentes fórmulas, se ha intentado en los últimos años gravar todas y cada una de las acciones que integran el circuito económico del Bitcoin —o de cualquier otra 'moneda virtual'—, lo que incluye actividades que van desde su obtención, a través de la operación denominada "extracción" o "minado" (ya veremos más adelante en qué consiste); su mera tenencia en el tiempo, como si se tratara de una especie de instrumento financiero; y hasta su intercambio bajo la modalidad de compra-venta con otros activos de naturaleza similar o dinero de curso legal.

Ahora bien, el mundo de la actividad criminal no ha sido ajeno a estos cambios. La expansión que se advierte en el conocimiento —y en menor medida, el uso cotidiano— del Bitcoin por parte del grueso de la sociedad, también ha tenido su correlato en el campo de la delincuencia, tanto de carácter organizada como, incluso, en aquella menos sofisticada. Allí se verifica un incremento notable en su utilización, lo cual puede responder a varios factores, entre ellos, la supuesta característica de anonimato que se le atribuye, la facilidad y velocidad que ofrece en materia de flujo e intercambio de fondos —lo que permite su disponibilidad en segundos en cualquier parte del mundo, sin necesidad de recurrir a un traslado físico ni al auxilio de una institución financiera—, y, obviamente, conectado con esto último, la amplitud de mercado y diversidad de opciones que ha experimentado su acceso y comercialización.

Para ser más gráfico, el uso del Bitcoin se ha presentado en la ejecución de conductas delictivas de las más diversas, que ya no necesariamente se circunscriben al entorno digital. En su momento fueron novedad casos de extorsiones complejas en las que se exigían pagos por esta vía, como, por ejemplo, aquellas denominadas bajo el nombre de *ransomware* o *sex-extortion* **(4)**; o casos en los que se utilizaba al Bitcoin como moneda de cambio para comercializar en la *deep web* **(5)** sustancias, objetos e imágenes de carácter ilícito, e incluso hasta datos sensibles de particulares, empresas privadas y agencias públicas. Ni que hablar de maniobras de fraude, de distintas características, que finalizaban con transacciones a través de esta criptomoneda.

Sin embargo, hoy su utilización se ha extendido a una criminalidad mucho más burda. Desde la contratación de un sicario hasta el pago de un rescate en un caso de secuestro extorsivo. Es evidente que se busca aprovechar la 'distancia física', 'reserva de identidad' y facilidad de comercialización que ofrece esta 'moneda virtual'. Qué mejor para el/la delincuente que evitar atravesar los riesgos ínsitos de un desembolso dinerario realizado en forma presencial o a través de los canales financieros ordinarios.

Incluso han salido a la luz reportes elaborados por agencias estatales de investigación de carácter internacional **(6)** en los que se ha advertido sobre la utilización del Bitcoin —así como de otras cripto-monedas, aunque en una menor medida— por parte de organizaciones delicti-

---

nes y de seguimiento de activos en una red de negocios" - cfr. https://www.ibm.com/ar-es/topics/what-is-blockchain.

(3) El reporte publicado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en el año 2020, denominado "Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues", ofrece un amplio relevamiento sobre el estado de situación en materia de tributación de 'cripto-activos' en el que se encuentran una gran cantidad de países.

(4) Básicamente, un ransomware consiste en una maniobra mediante la cual los delincuentes logran tomar control de un sistema informático, archivos o conjunto de datos, los encriptan volviéndolos inaccesibles y exigen a su dueño un pago como 'rescate', esto es, para su liberación y devolución. Por su parte, una maniobra de sex-extortion consiste en chantajear a una persona con la amenaza de difundir una imagen o vídeo de sí misma realizando algún acto sexual, o bien encontrándose en alguna situación de intimidad.

(5) Lo que se conoce como "internet profunda", esto es, cuyo contenido no puede ser indexado por los grandes buscadores como Google, Bing, Yahoo, etc.

(6) Cfr. informe titulado "2018 - National Drug Threat Assessment", emitido en el mes de octubre del año 2018 por la Drug Enforcment Administration (DEA), US Departament of Justice, ps. 126-130 —link descarga: https://www.dea.gov/documents/2018/2018-10/2018-10-02/2018-national-drug-threat-assessment-ndta—.

vas como medio para ocultar, resguardar y trasladar dinero proveniente de actividades ilícitas; es decir, hablamos de su empleo, ya no para materializar la maniobra delictiva en sí, sino en lo que sería el paso posterior, como refugio o vía para atesorar o movilizar la ganancia, o bien para dar inicio a su proceso de blanqueo. A ello se le suma la preocupación mundial por su utilización como canal para financiar "operaciones de grupos terroristas" **(7)**, a través de donaciones anónimas fomentadas por campañas desplegadas en diversas redes sociales.

En definitiva, el uso de esta cripto-moneda en el ámbito de la actividad criminal pareciera no tender a expirar, sino más bien, todo lo contrario. Es plausible prever una expansión en el futuro que impacte en este campo cada vez con mayor fuerza. La situación se agrava, como se dijo, a poco que se advierta la aparición constante y el empleo de nuevas formas de activos digitales —criptomonedas, tokens—, cada uno con sus propias características de creación, funcionabilidad y comercialización y, por ende, también de abordaje **(8)**.

El escenario descripto —y más aún la proyección sobre su evolución— obliga inmediatamente a pensar qué respuesta se puede dar desde el lado opuesto a la criminalidad, es decir, cómo deben prepararse las agencias estatales encargadas de la persecución penal y los órganos de justicia para hacer frente a un caso de estas características. ¿Es posible diagramar una estrategia de investigación seria que permita su abordaje con alguna posibilidad de éxito? ¿Cómo planificar la acción en materia cautelar cuando se está frente a activos de esta naturaleza?

Precisamente, sobre ambos ejes se centra el objetivo buscado con la elaboración de este trabajo. La idea no es desarrollar en profundidad los conceptos técnicos y teóricos que rodean al Bitcoin —sobre lo cual ya hay mucho escrito y de calidad—, sino en dotar al lector de los conocimientos básicos y las herramientas necesarias para que pueda emprender tales cometidos con la mayor eficiencia posible, a sabiendas de su importancia y trascendencia para el correcto funcionamiento del sistema de justicia penal.

Bajo ese norte, en la primera parte se abordarán algunas nociones esenciales sobre el funcionamiento de la red y se describirá la inserción que presenta esta cripto-moneda en el mundo físico-digital actual. Como paso siguiente, se explicará de qué manera realizar una lectura amplia y correcta de las transacciones, que permita extraer de ellas toda información que pueda ser de relevancia para el avance de un caso. Ello incluye desde poder ubicarlas en la *blockchain* y hacer el seguimiento de las unidades de valor comprometidas —reconstruir el flujo y destino final de los fondos—, hasta determinar en qué otras operaciones participaron las *billeteras virtuales* involucradas.

También se desarrollarán los aspectos principales de una metodología de actuación que, bajo ciertas circunstancias, puede ser empleada para intentar individualizar a la persona que está detrás del manejo de una cartera específica. Como se verá, su correcta implementación exigirá no solo conocer el funcionamiento y los servicios que ofrecen las plataformas más importantes del ecosistema Bitcoin, sino también contar con un canal de comunicación ágil y certero con las empresas que las administran, de forma tal de poder formulares requerimientos de información sobre sus usuarios.

Por último, se trazarán algunos lineamientos que, desde mi parecer, deben ser tenidos en consideración a la hora de proyectarse la ejecución de cualquier medida de índole cautelar. Conforme se detallará, la tenencia de sumas de bitcoins se puede materializar bajo modalidades bien distintas (ej.: desde ser uno responsable de su custodia en un dispositivo propio, hasta delegar dicha tarea en una empresa que provea tal servicio), por lo que las posibilidades de incautación dependerán, básicamente, de que se adopte un curso de acción acorde al escenario particular que se presente.

(7) Cfr. Directiva (UE) 2018/843 emitida por el Parlamento Europeo y el Consejo de la Unión Europea en fecha 30 de mayo de 2018.

(8) No obstante, los informes especializados en la materia siguen ubicando al Bitcoin en una posición de predominio por sobre el resto de las 'monedas virtuales', al punto que se destaca su utilización, en muchos casos, como vía primaria de acceso o adquisición de aquellas.

Como cierre de la introducción, no quería dejar de señalar que detrás de la elaboración de este trabajo también fluye la idea de que opere como una especie de incentivo para los propios destinatarios, en el sentido de generar la discusión sobre las interpretaciones y herramientas que aquí se proponen, y que ello derive en la búsqueda y el desarrollo de canales de abordaje aún más completos y útiles. Es innegable que se trata de una temática con notable vigencia, pero sobre la que poco se ha profundizado en el ámbito de la doctrina procesal-penal. Esperemos, entonces, que sirva de puntapié inicial y pueda ser mejorado en un futuro cercano con novedosos aportes.

II. Desarrollo

II.1. Qué es el bitcoin y cómo funciona su red

La primera pregunta no es fácil de responder y de hecho aún hoy genera un sinfín de discusiones y posiciones encontradas, tanto en nuestro país como en el extranjero. Si bien se ha enmarcado al Bitcoin en lo que popularmente se denomina como 'moneda virtual' o 'criptomoneda', las diferencias aparecen a la hora de hilar más fino e intentar dilucidar concretamente en qué categoría jurídica debe encuadrarse este nuevo concepto. El punto de discordia no es menor ya que impacta de lleno en varias esferas legales, como ser, entre otras, el tratamiento fiscal a aplicarse o las regulaciones a las que podrían quedar sometidas tanto sus operaciones como los actores que participan en ellas —ej.: 'transacciones financieras', 'protección al consumidor', etc.—.

Las definiciones que se han ensayado al respecto, desde distintos ámbitos, se presentan de lo más diversas. A modo de ejemplo, se ha llegado a catalogar al Bitcoin como un "activo patrimonial inmaterial en forma de unidad de cuenta", o bien como "un sistema de pago *alegal*". Incluso se le ha asignado carácter de 'bien digital'. La falta de uniformidad en este aspecto es manifiesta y se replica hasta en informes o disposiciones emitidas por organismos intergubernamentales de carácter internacional **(9)**.

En Argentina aún no se ha dictado una regulación específica sobre la temática que ponga punto final a la controversia. De hecho, han sido pocas las agencias estatales que, por medio de documentos oficiales, intentaron dar respuesta a este problema de conceptualización. El antecedente más importante lo constituye la res. 300/2014 emitida en el mes de julio del año 2014 por la Unidad de Información Financiera. Se trataba de una directiva dirigida a los 'sujetos obligados' enumerados en la ley 25.246 de Entidades Financieras para que prestaran "especial atención al riesgo" que implicaban "las operaciones efectuadas con monedas virtuales". En ella, explícitamente se definió a estas últimas como "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" **(10)**. No obstante, vale aclarar, su alcance se limitaba a dicho ámbito de actuación.

Para la misma época, el Banco Central de la República Argentina publicó un comunicado en su sitio web oficial **(11)**, dirigido al público en general, en el que además de alertar sobre los riesgos implícitos en el uso de las "monedas virtuales", formuló ciertas aclaraciones sobre su acción constitutiva. Concretamente, enfatizó que no eran emitidas por la entidad ni por otras autoridades monetarias internacionales y que, por lo tanto, carecían de curso legal y/o respaldo alguno. Si bien no las enmarcó en ninguna categoría jurídica, dejó en claro los

(9) Cfr. el artículo "La Tributación del Bitcoin", publicado en la Revista Quincena Fiscal, N° 1-2, año 2022, escrito por el reconocido Profesor de la Universidad de Castilla-La Mancha (Toledo, España), Dr. Luis María Romero Flor, en el cual realiza un repaso minucioso sobre las distintas conceptualizaciones con las que se ha intentado definir al Bitcoin, así como también el tratamiento legal dispensado.

(10) Tal definición buscó ir en línea con las recomendaciones formuladas por el Grupo de Acción Financiera Internacional (GAFI) a través del reporte denominado "Virtual Currencies. Key Definitions and Potential AML/CFT Risks", emitido en el mes de junio de ese mismo año.

(11) https://www.cronista.com/infotechnology/internet/El-Banco-Central-argentino-considera-riesgoso-operar-con-bitcoins-20140528-0003.html.

elementos que las diferenciaban de cualquier moneda fiduciaria **(12)**.

En los años siguientes, al menos en nuestro país, ningún cambio sustancial se produjo. Pese a que la ley 27.430, sancionada en el año 2017 y modificatoria de Ley de Impuesto a las Ganancias, incorporó como hecho imponible los beneficios derivados de la enajenación de "monedas digitales", nada dijo sobre su conceptualización y/o tratamiento legal aplicable.

En definitiva, la respuesta a la pregunta sobre qué es el Bitcoin, no la vamos a encontrar en el plano normativo —y menos aún, como se expuso, de manera uniforme—. Ello nos obliga a dejar a un lado el problema de su definición legal e intentar abordar la cuestión desde una perspectiva distinta, enfocada principalmente en el uso que se le puede dar y las características que exhibe el funcionamiento de su red. Como se verá a continuación, no es casual el hecho de que se lo catalogara como una "cripto-moneda".

Comencemos por el uso. ¿Qué puedo hacer con bitcoins hoy? La respuesta es sencilla. Exactamente lo mismo que puedo hacer con cualquier moneda de curso legal (pesos argentinos, dólares estadounidenses, euros, según el lugar del planeta en que me encuentre) pero a una escala todavía menor.

En tal sentido, si lo deseo, puedo usar bitcoins para comprar bienes o pagar servicios, tanto en el mundo digital como físico. A modo de ejemplo, ya hay una gran cantidad de plataformas online que lo aceptan como medio de pago. A través de ellas se puede adquirir desde un electrodoméstico o indumentaria deportiva, hasta un pasaje aéreo hacia el exterior; o abonar por algún servicio informático, como la registración de un dominio en internet, el servicio de alojamiento web de un sitio o la contratación de una red VPN, entre otros.

Incluso ya hay restaurantes y hoteles ubicados en la Ciudad de Buenos Aires que aceptan pagos en bitcoins. Uno puede ir, sentarse a almorzar y pagar la comida a través de este medio; u hospedarse y abonar de idéntica forma el alojamiento. Hasta fue noticia dos veranos atrás la aparición de un balneario en la ciudad costera de Pinamar que aceptaba bitcoins como medio de pago para el alquiler de carpas y sombrillas.

Vale aclarar, igualmente, que por el momento son pocos los locales comerciales que lo han implementado. No obstante, existen varias plataformas que se dedican, precisamente, a masificar el uso del Bitcoin, ofreciéndole a los distintos comercios, sin importar el rubro, un sistema de procesamiento de pagos a través del cual poder incluirlo dentro de las opciones de cobro. Esta práctica, que aún no ha tenido gran desarrollo en nuestro país, exhibe niveles de mayor expansión en algunas ciudades del exterior (por ejemplo, en la zona comercial de Akihabara, en plena ciudad de Tokio, muchas tiendas electrónicas aceptan el Bitcoin como medio de pago).

En la misma línea, también han aparecido varios emprendimientos que pusieron el foco en facilitarle al cliente el uso del Bitcoin para transacciones diarias. Por ejemplo, emitiendo una especie de 'tarjeta de débito' con la cual poder realizar pagos en moneda fiduciaria (según el caso, pesos argentinos, dólares estadounidenses, etc.) pero respaldada con sumas de bitcoins almacenadas en cuentas abiertas dentro de la respectiva plataforma.

Sin embargo, el uso del Bitcoin no se limita a la mera posibilidad de comprar bienes o pagar servicios. También puede ser intercambiado con monedas de curso legal, como lo es el dólar estadounidense o el peso argentino. En tal sentido, existen varios sitios web que funcionan como "casas de cambio" online y cotizan el Bitcoin como si fuese una moneda más; es decir, ofrecen la compra o venta de bitcoins a precio comparativo con las mencionadas divisas.

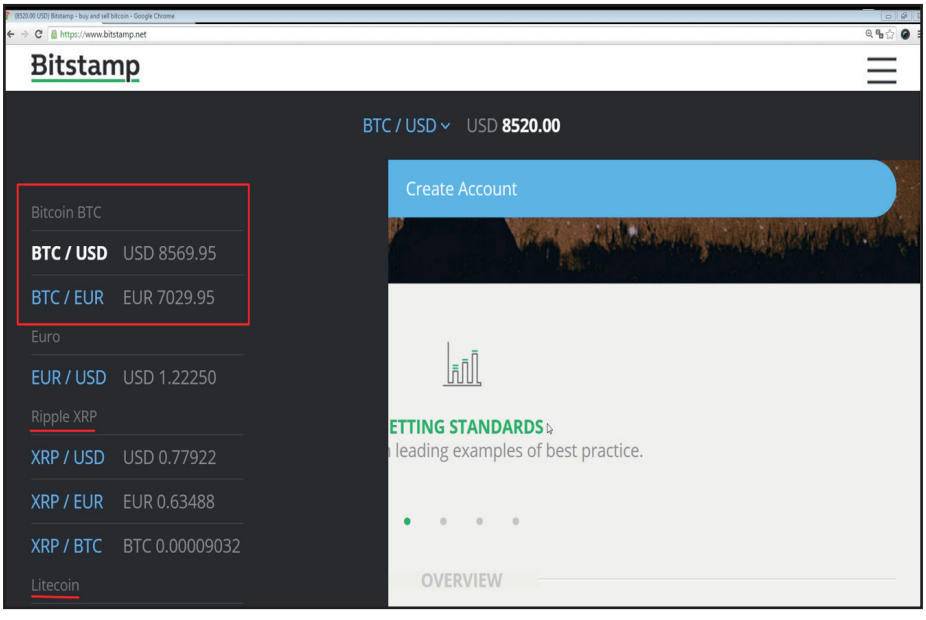
Básicamente, uno puede ingresar en ellos y vender bitcoins que estén en su poder, llevándose a cambio el monto equivalente en alguna moneda legal; o al revés, depositar sumas de pesos o dólares y retirar el monto equivalente en bitcoins. La mayoría de estos sitios, además, incluyen dentro de su oferta la posibilidad de "intercambiar" los bitcoins por alguna otra de

(12) Un comunicado de características similares fue emitido por el organismo en fecha 20 de mayo de 2021, en conjunto con la Comisión Nacional de Valores —cfr. http://www.bcra.gov.ar/Noticias/alerta-sobre-riesgos-implicancias-criptoactivos.asp

las denominadas cripto-monedas (Litecoin, Ether, XRP, etc.), a las cuales cotizan y comercializan de idéntica forma.

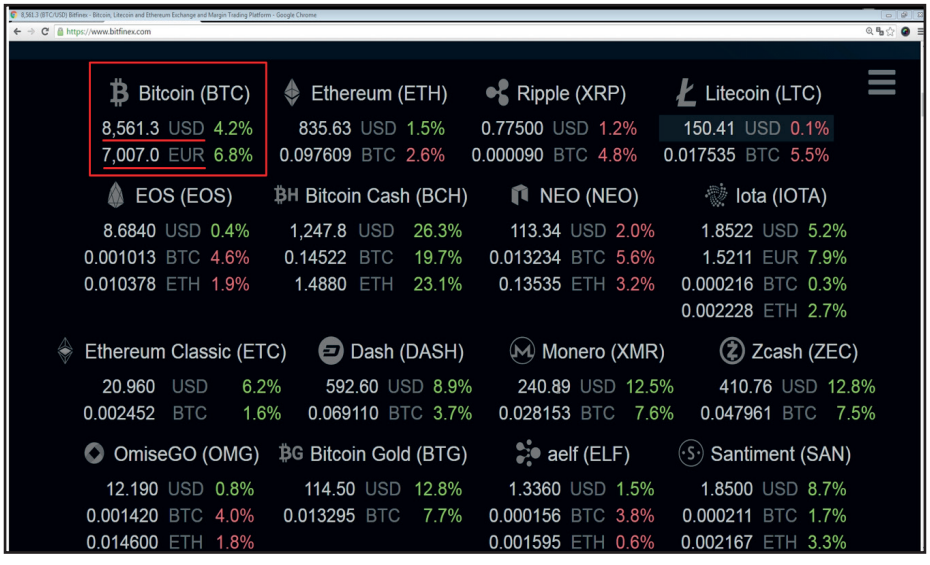
Cabe resaltar que las características del servicio que brindan estas plataformas, esto es, los medios de pago ofrecidos, las comisiones impuestas por cada transacción, las divisas aceptadas, las vías o limitaciones de retiro del capital y los requisitos exigidos para operar, varían según cada una de ellas y hasta pueden verse influenciadas tanto por el país en que se encuentran radicadas como aquel desde el cual actúan los usuarios **(13)**.

Las imágenes que se muestran a continuación reflejan cómo se exhibe en algunos de estos sitios la cotización del Bitcoin o la de alguna otra denominada cripto-moneda, la cual puede verse modificada segundo a segundo.

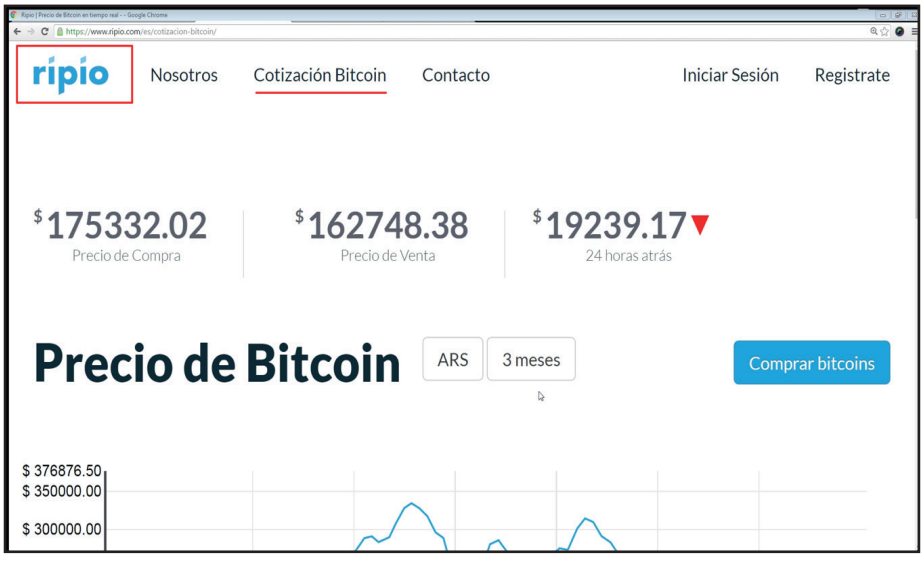


www.bitstamp.com

(13) A modo de ejemplo, la Directiva 2018/243 emitida por parte del Parlamento Europeo y el Consejo de la Unión de Europa, relativa a la "prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo", posiciona como 'Sujetos Obligados' a aquellas compañías que, en el ámbito de la Unión Europea, operen como proveedoras de servicios de cambio de monedas virtuales por monedas fiduciarias, o bien de custodia de monederos electrónicos. Por consiguiente, les exige cumplir con las obligaciones de 'Diligencia Debida' con respecto a determinados clientes, entre las cuales se encuentra la de su correcta identificación, la evaluación y obtención de información sobre el propósito de una operación o la índole de una relación de negocio, y hasta la aplicación de medidas de seguimiento o escrutinio de transacciones (cfr. arts. 2.3.g y 13).



www.bitfinex.com



www.ripio.com (esta web cotiza el precio del bitcoin en pesos argentinos y brinda muchas facilidades para su compraventa).

Es importante aclarar que este tipo de operaciones (intercambiar sumas de bitcoin por unidades de valor de alguna moneda de curso legal, o mismo de alguna otra cripto-moneda) pueden ser realizadas, tranquilamente, sin necesidad de recurrir a este tipo de plataformas; es decir, dos personas, sentadas frente a frente en un bar o separadas por kilómetros de distancia, llevando consigo los dispositivos a través de las cuales administran sus respectivas billeteras digitales, pueden materializar la transacción sin ninguna dificultad. De hecho, existen foros o grupos en redes sociales que operan

como lugares de 'encuentro' para que se conecten entre sí eventuales compradores y vendedores **(14)**.

Hasta aquí, pareciera ser que el uso que se le puede dar al Bitcoin no deja espacio para muchas dudas; al menos desde lo fáctico, podemos decir que estamos frente a una especie de moneda virtual que, aún sin ser de curso legal, es decir, sin ser emitida ni autorizada por la respectiva autoridad gubernamental (en nuestro caso, el Banco Central de la República Argentina), es aceptada y utilizada voluntariamente dentro de un mercado pequeño, con foco principalmente en la web, que tiende a expandirse cada vez más. A su vez, como tal, puede ser fácilmente intercambiado por divisas que, a diferencia suyo, sí tienen una circulación autorizada y operan como monedas fiduciarias (pesos argentinos, dólares estadounidenses, euros). Ello, naturalmente, lo vuelve muy atractivo para el mundo de la actividad criminal.

Ahora bien, ¿por qué hablamos de cripto-moneda? Esta pregunta nos lleva directo a meternos en lo que es el funcionamiento de su red. Intentemos una primera aproximación, con la advertencia al lector de que hay conceptos que recién podrán ser apreciados con mayor claridad una vez que avancemos, a través del uso de imágenes y ejemplos, en el análisis de cómo se desarrollan las transacciones y las búsquedas en la blockchain ("cadena de bloques") **(15)**.

La principal característica del Bitcoin, más allá de la innovación que implica el hecho de que sus unidades de valor no tengan soporte físico de ningún tipo, es que su funcionamiento no está sujeto al control y respaldo de una institución central, es decir, no hay una autoridad responsable de su emisión y puesta en circulación. Por el contrario, funciona en forma descentralizada a través de una red electrónica de pares denominada *peer to peer* (P2P), la cual no solo utiliza técnicas de criptografía para procesar y registrar las transacciones, sino que, además, es controlada por sus propios usuarios **(16)**.

Básicamente, a través de la mencionada tecnología blockchain se estructuran secuencial y cronológicamente todas las transacciones que acontecen en la red, creándose una especie de registro global y único de ellas, de carácter permanente y público, que puede ser accedido para su visualización por cualquiera que lo desee (como si se tratase de un gran libro contable). Esta base de datos se va retroalimentando y es compartida por todos los nodos de la red, es decir, por todos aquellos equipos informáticos que, a la manera de "pares" o "iguales", participan en ella y le brindan algún tipo de soporte, lo que vuelve computacionalmente muy difícil, para no decir inviable, su modificación.

La transferencia de bitcoins se concreta, simplemente, renunciándose a su posesión. Cada usuario que participa en la red posee una especie de *billetera digital* en la que resguarda juegos de llaves criptográficas, públicas y privadas, en las que se enlazan las respectivas unidades de valor. La dirección pública actúa como punto receptor del pago. La privada, en cambio, sirve para autorizar el traspaso. Una vez que este se concreta, lo que ocurre no es más que una reasignación del poder de disposición sobre las unidades transferidas (en el punto siguiente veremos este tema con mayor profundidad).

La información de la transacción se transmite a toda la red, la cual previo a aceptar su validez, esto es, incluirla en un bloque y añadirlo a la cadena existente, verifica por medio de una operación algorítmica la autenticidad de las llaves involucradas y la disponibilidad de las unidades de valor enviadas. Este proceso de validación se

(14) Hay sitios web (por ejemplo, www.LocalBitcoins.com) que, además de contactar entre sí eventuales compradores y vendedores, actúan directamente como un intermediario formal de la transacción. Desde una posición de 'garante', retienen la suma de bitcoins hasta tanto ambas partes hayan confirmado la concreción del pago acordado.

(15) Igualmente, si es del interés del lector introducirse con mayor profundidad en los conocimientos técnicos detrás del funcionamiento de la red Bitcoin, recomiendo la lectura del libro "Mastering Bitcoin", escrito por Andreas M. Antonopoulos. Asimismo, para una visión más orientada a su posible impacto en el futuro de la economía y la escalabilidad en su uso para transacciones diarias, la mejor opción es el libro "El Patrón Bitcoin", escrito por Saifedean Ammous.

(16) Esto es muy importante tener presente a la hora de dirigir una investigación penal. Así como no hay ningún servidor o punto de control 'centralizado' en el que se almacene toda la información de la red, tampoco hay una autoridad responsable que la maneje o coordine, a la que eventualmente se pueda recurrir para requerir información sobre sus usuarios y/o transacciones.

denomina “minería” y es llevado adelante por nodos especiales que, para dicha labor, ponen a disposición una gran cantidad de esfuerzo computacional. A cambio de ello, por cada bloque generado y añadido a la cadena, se los recompensa con una determinada suma de bitcoins ya establecida previamente. Este incentivo hacia los “mineros”, precisamente, es la forma novedosa que adopta el Bitcoin para crear y poner en circulación sus unidades de valor. El número máximo de creación ya está fijado en 21 millones de bitcoins.

Es importante aclarar que los “mineros”, además, pueden recibir como recompensa una comisión por cada transacción validada e incluida en el bloque añadido, la cual es asumida y fijada por el propio usuario transferente. Aquellas operaciones que mayor monto ofrezcan en tal concepto van a ser confirmadas en un orden prioritario. La red está programada de forma tal que, cada diez minutos aproximadamente, se incorpore a la cadena un bloque con un nuevo grupo de transacciones **(17)**.

II.2. Cómo operar en la red Bitcoin

Formulada ya una explicación general sobre su funcionamiento, se intentará en este punto profundizar respecto de cómo se desarrollan las operaciones con bitcoins, usando como eje la perspectiva del usuario, es decir, enfocándonos en qué elementos necesita uno para operar y cuáles son los pasos que se deben seguir.

II.2.a. 'Direcciones bitcoin' y 'billeteras virtuales'

Lo primero que hay que saber es que los bitcoins no tienen similitud con los billetes de papel que conocemos y utilizamos en nuestra vida diaria. A diferencia de estos, no se identifican con un número, ni con un código. Por eso la expresión “tengo tal bitcoin” es equivocada, no refleja la realidad. Las que llevan identificación son las direcciones públicas a las que hicimos referencia antes, en las que se enlazan las respectivas sumas de bitcoins **(18)**. Pensando en una analogía para intentar formarnos una mínima representación de ellas, podríamos decir que son como una especie de recipientes en los que se almacenan unidades de bitcoins, cada uno de los cuales está cerrado con un candado cuya llave (la clave privada asociada a la dirección) es la que permite a su dueño —o a quien tenga acceso a la misma— liberar los fondos y disponer de ellos.

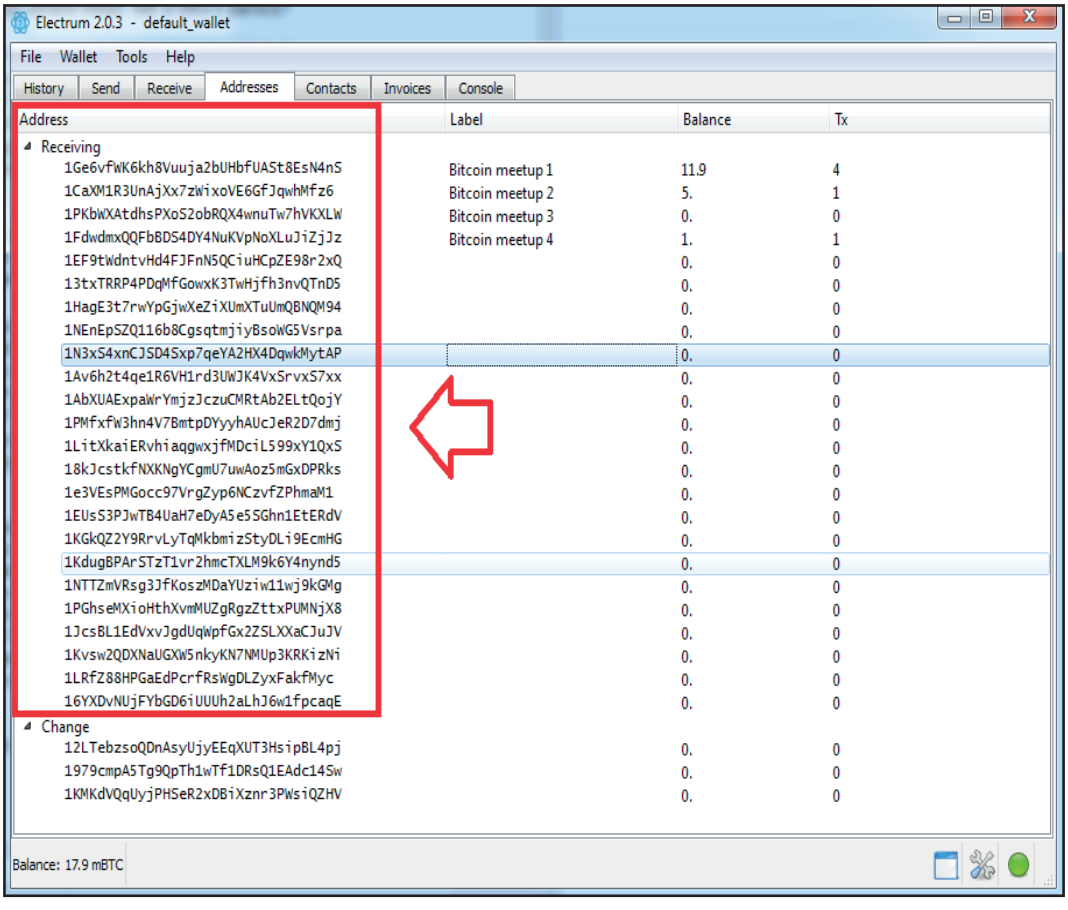
Estas direcciones se identifican con una cadena alfanumérica de, por lo general, 33 caracteres, aunque ese número puede variar (incluso pueden presentarse en formatos distintos, como un código QR). La imagen que se muestra a continuación refleja cómo se visualiza una dirección Bitcoin.

(17) Se dice que una transacción queda completamente confirmada —y ya no hay dudas de su autenticidad— una vez que el bloque que la añadió a la 'cadena' queda enterrado debajo de 4 o 6 bloques incorporados con posterioridad, lo que implica aguardar, al menos, entre 40 y 60 minutos de tiempo. Este punto configura, al igual que el alto valor de la 'comisión' a incluir en la transacción, uno de los tantos problemas que se visualiza hoy en torno a la posibilidad de su escalabilidad para operaciones diarias.

(18) Es importante tenerlo en cuenta por si el día de mañana, en el marco de una investigación, realizamos un procedimiento en el que vamos a buscar algún rastro de una transacción puntual o recabar información sobre los movimientos que pudo haber materializado en la red un usuario en particular.

Si bien estas 'direcciones bitcoin' que actúan como punto receptor de un pago suelen ser asociadas con las llamadas 'billeteras virtuales', es importante aclarar que no son lo mismo. Se trata de cosas distintas, aunque estén íntimamente vinculadas. Las 'billeteras virtuales' (también conocidas como 'carteras' o 'monederos' digitales) no son más que programas que permiten generar y gestionar uno o más de ese juego de llaves criptográficas, conformado, precisamente, por la propia dirección pública y su respectiva clave privada. Es decir, actúan como interfaz para operar sobre la red, permitiéndole al usuario gestionar las distintas direcciones que la componen y enviar o recibir bitcoins a través de ellas.

La imagen que se exhibe a continuación refleja cómo se visualiza en una misma 'billetera digital' las distintas direcciones Bitcoin que la integran.



La imagen corresponde a una cartera denominada “Electrum”

Existen varios modelos de billeteras y cada una presenta funcionalidades distintas, las cuales pueden variar en torno a diversos tópicos, como ser seguridad, privacidad, facilidad de uso, etc. Algunas de ellas consisten en programas que se instalan en computadoras de escritorio y/o portátiles, y se destacan por permitir al usuario *mantener un control absoluto de los fondos almacenados,* ya que es él quien resguarda las claves privadas de las direcciones asociadas y, por ende, quien puede habilitar su desbloqueo **(19)**. Según el caso, operan como un nodo completo de la red (almacenando y actualizando constantemente una copia entera de la *blockchain*), o bien desde una posición externa con respaldo en uno de ellos, a través de un sistema de validación simplificada, lo que los vuelve más ligeros y accesibles. Entre las más conocidas se destacan "Bitcoin Core" y "Electrum".

Otro modelo de 'billetera' es el que se brinda, regularmente, a través de plataformas web o aplicaciones móviles. Las empresas que las administran ofrecen a los usuarios el servicio de custodia y manejo de sumas de bitcoins. Básicamente, le garantizan su cuidado y se encargan de ejecutar todas las operaciones que aquel disponga (funciona como una cuenta abierta en un banco). Por lo general, cobran una comisión por cada transacción y presentan una interfaz sumamente amigable, en la que quizás no haya que recordar más que una sola contraseña general. De hecho, se destacan por facilitarle al cliente la disposición de los fondos de manera rápida, sencilla y sin importar el lugar físico en que se encuentre. Ello las convierte en las más elegidas dentro del ecosistema Bitcoin, pero lo cierto es que son las que menos seguridad ofrecen. Es que el usuario debe *delegar en el proveedor del servicio el control de los bitcoins*, como sucede en nuestra vida diaria con los fondos que se depositan en una institución bancaria. Por ello es necesario confiar en su honestidad **(20)**. Entre las más utilizadas en la actualidad, se destacan las carteras ofrecidas por empresas como "Binance", "CoinBase", "Xapo" y Bitstamp", las cuales, vale aclarar, también ofrecen el ya mencionado servicio de *exchange* (intercambio por monedas fiduciarias u otras cripto-monedas) **(21)**.

Por último, están los dispositivos físicos diseñados específicamente para almacenar claves privadas que, según el caso, pueden o no tener funcionalidades operativas (de hecho, un papel con la respectiva anotación puede cumplir esa misma tarea). Generalmente se los utiliza para guardar grandes sumas de bitcoins y se los mantiene "congelados" en el tiempo, es decir, se intenta no concretar ninguna operación a través de ellos, ya que al estar completamente aislados de toda conexión a internet están menos expuestos a posibles ataques y/o

(19) Cabe aclarar, igualmente, que la mayoría de las billeteras están configuradas de forma tal que el usuario, a la hora de operar, no tenga que estar colocando la clave privada de cada dirección involucrada en la transacción a realizar; e incluso, para el caso en que por una cuestión de seguridad o con motivo de un infortunio, necesite regenerar la billetera en otro equipo o migrar las direcciones hacia otra cartera (en el mundo Bitcoin, a esta última acción se la conoce como "exportar direcciones"), algunas utilizan un esquema de derivación de claves privadas que le permiten a aquél evitar tener que recordar o registrar cada una de ellas, con las dificultades que ello conlleva, en función de la gran cantidad de caracteres que las componen, y trabajar únicamente con una "clave maestra" - más conocida como semilla— conformada aleatoriamente por doce palabras. Otras, directamente, crean en el propio equipo una copia de seguridad (backup) de las respectivas claves privadas.

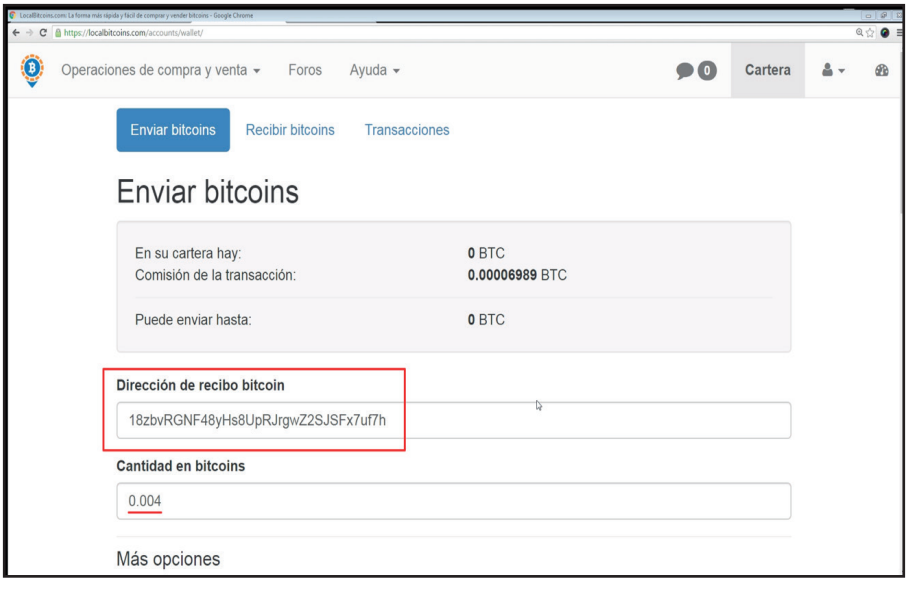
(20) A lo largo de los años, desde la creación del Bitcoin, ha ocurrido muchas veces que plataformas web que ofrecían el servicio de "billetera online" resultaron hackeadas y sufrieron la sustracción de los fondos almacenados por los usuarios, no pudiendo responder ante ellos frente a semejante perdida. El caso más conocido tuvo lugar en el año 2014 y fue el del broker MtGox.com, radicado en la ciudad de Tokyo, Japón, cuyas pérdidas ascendieron a la suma de 850.00 bitcoins (para ese momento, alrededor de 470 millones de dólares). También ha sucedido que ciertos sitios web, tras generar confianza en la comunidad y atraer clientes a partir del ofrecimiento de determinados beneficios (ej. retornos dinerarios en función del 'cuidado' temporal de los bitcoins), repentinamente dejaron de estar en línea y desaparecieron por completo del mapa, perdiendo los usuarios las sumas allí depositadas.

(21) Uno puede acceder a esos sitios web —o descargar sus aplicaciones móviles—, crearse una cuenta y adquirir unidades de valor tanto de Bitcoin como de alguna otra cripto-moneda, las cuales podrá almacenar en la propia 'billetera' que la plataforma ofrece y, desde allí, ejecutar todas las operaciones que desee (enviar bitcoins a una cartera externa, brindada por otra compañía; recibir bitcoins provenientes de ella; efectuar cambios por monedas fiduciarias; etc.). Entre las empresas argentinas más reconocidas que ofrecen este mismo servicio a través de plataformas web y/o aplicaciones móviles, sobresalen "Ripio", "SatoshiTango" y "ArgenBTC".

vulneraciones, lo que les otorga mayor seguridad. Los más conocidos en el mercado son los dispositivos "Trezor" y "Ledger".

Ya veremos más adelante como los distintos modelos de 'billeteras' que pueden ser utilizados para operar en la red impactan de lleno en lo que es la actividad cautelar, por lo que es sumamente importante conocer cómo se opera a través de cada una de ellas y qué funcionalidades presentan, de forma tal de poder trazar una correcta planificación de dicha medida procesal.

La imagen que se muestra a continuación refleja cómo se visualiza, desde la óptica de un usuario, una 'billetera virtual' brindada por una plataforma web (en este caso www.LocalBitcoins.com).



II.2.b. Transacciones

Como primer punto, es importante destacar que los bitcoins no son unidades fijas que se van moviendo de una dirección a otra; es decir, si yo recibo en una dirección una determinada suma de bitcoins, mi transacción siguiente no va a tener que ser, necesariamente, una única transferencia por ese mismo monto —aunque puede serlo—. En ese sentido, hay que tener presente que los bitcoins *pueden fraccionarse en unidades más pequeñas* hasta llegar a los ocho decimales (la mínima unidad se denomina "satoshi" y se expresa con el siguiente valor: 0.00000001 BTC) **(22)**. De allí que sea posible, si uno lo desea, partir un monto que se recibe, conservar tan solo una parte de aquel y transferir el resto a otras direcciones bitcoin por medio de varias operaciones distintas, concretadas en días, horas, minutos y hasta segundos diferentes.

Veámoslo con un ejemplo. Si uno recibe en una dirección ("A") la suma de 5 bitcoins, así como puede transferir esa misma cantidad a otra dirección en una única operación, también tiene la opción de: fraccionar el monto, conservar en ella 3.2 bitcoins y transferir el resto de la siguiente manera: 1) una hora más tarde, la suma de 1.2 bitcoins hacia la dirección "B"; 2) al otro día, la suma de 0.4

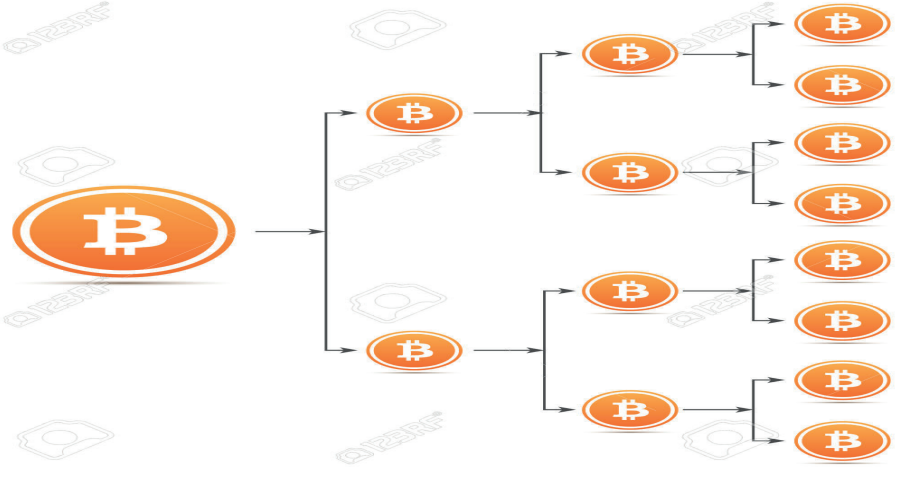
(22) También suele utilizarse como medida el término mBTC, que representa lo que sería una milésima de un bitcoin (1mBTC sería igual a 0.001 BTC).

bitcoins hacia la dirección "C"; 3) y tan solo unos minutos después de que se concretara esta última operación, la suma de 0.2 bitcoins hacia la dirección "D" **(23)**.

A la par de ello, también hay que tener en cuenta que *las direcciones bitcoin no tienen limitación de uso alguna* y, por lo tanto, puede enviarse hacia ellas la cantidad de bitcoins que uno desee, en tantas operaciones como se estime conveniente. Los montos que se reciban irán integrándose a la suma de bitcoins que ya estaba enlazada en la respectiva dirección; y se podrá disponer de su totalidad de idéntica forma a la ya expuesta, esto es, tanto en una única vez por medio de una sola operación, como fraccionándose a gusto, sin ningún tipo de restricción —ni en cantidades, ni en número de operaciones, ni en direcciones de destino—.

Siguiendo con el ejemplo anterior, si en la dirección de recepción ("B") a la que se envía la suma de 1.2 bitcoins, uno ya tenía enlazado un monto de 0.6 bitcoins —imaginemos, producto de dos transferencias distintas, concretadas en días anteriores por montos de 0.4 y 0.2 bitcoins, respectivamente—, se pasaría a tener en ella un total acumulado de 1.8 bitcoins. Este último monto, precisamente, podría transferirse en cualquier momento, en una sola transacción, a la dirección "C"; o bien podría partirse, conservarse en la dirección "B" la suma de 1 bitcoin y enviarse, en días u horarios diferentes, a las direcciones "C" y "D" el monto restante (podría ser 0.4 bitcoins a cada una de ellas, o bien elegirse cualquier otro tipo de fraccionamiento).

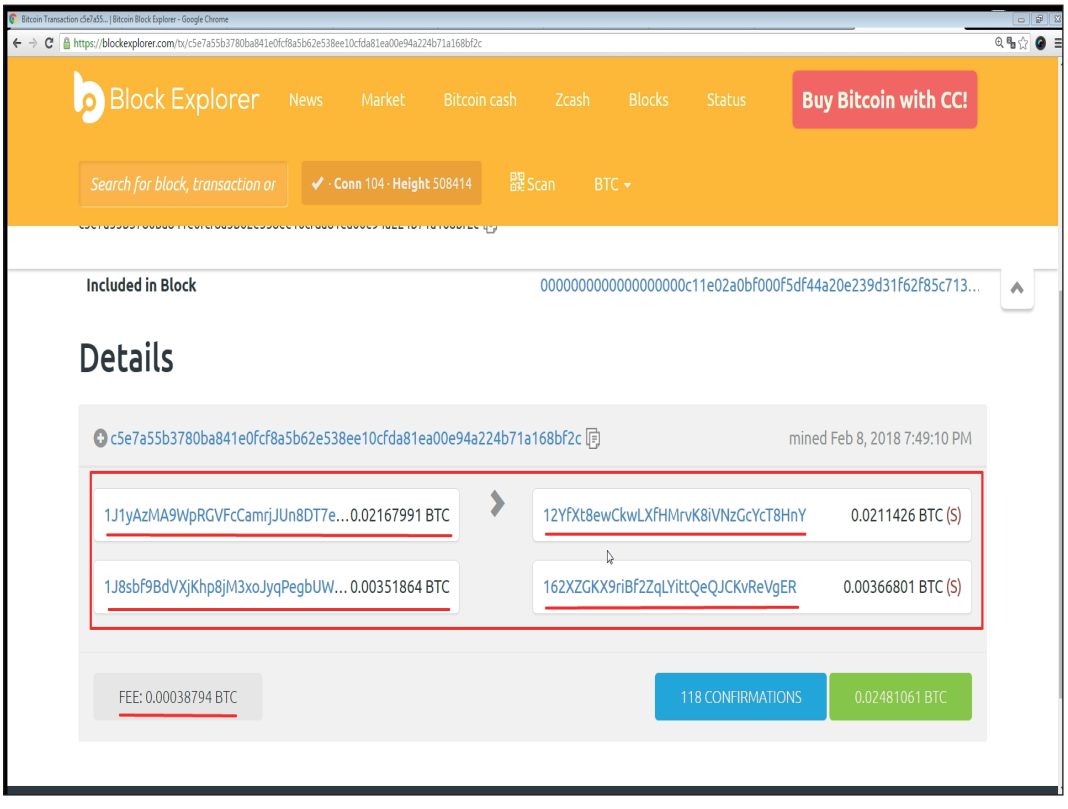
Ahora bien, ¿por qué es relevante marcar estas características que presentan las operaciones con bitcoins? Porque es muy probable que el día de mañana, cuando en el marco de una investigación intentemos seguir el rastro de una transferencia puntual, nos encontremos con un cuadro que exhiba una estructura gráfica similar a la de un árbol con muchas ramas; es decir, que la transacción inicialmente perseguida haya derivado en muchas operaciones subsiguientes, con una gran cantidad de direcciones Bitcoin involucradas y por montos hasta de los más diversos, quedando la suma enviada en un principio completamente licuada.



(23) Cabe aclarar que en un caso real los montos no resultarían así de exactos, ya que habría que descontar en cada transacción una comisión a pagar a los 'mineros' que la validen, integrándola por medio de un bloque a la cadena ya existente.

Una misma transacción, además, puede *incluir tanto múltiples direcciones de envío como de recepción.* En efecto, tal como se señaló, las propias 'billeteras virtuales' nos permiten gestionar las distintas direcciones que la integran y, de esa manera, los fondos que se enlazan en ellas. Así, en única operación, uno puede tomar unidades de bitcoins que están distribuidas en las distintas direcciones que componen la cartera y enviarlas, en la cantidad que decidamos, hacia una o más direcciones ajenas a la misma.

La imagen que se exhibe a continuación refleja con claridad lo marcado en el párrafo anterior. Corresponde a un sitio web que permite visualizar de manera completa la cadena de bloques de la red Bitcoin y muestra en particular una transacción en la cual, desde dos direcciones distintas, se enviaron unidades de bitcoins hacia otras dos direcciones diferentes.



No obstante, hay un detalle que debe ser tomado en consideración. Por la forma en que está configurada la red Bitcoin, las transacciones presentan un esquema particular de "entradas" y "salidas" que obligan al usuario transferente, en ocasiones, a tomar más unidades de bitcoins de las que desea enviar y por ello debe generar, para la restitución de ese sobrante, lo que se conoce como dirección de 'cambio' o 'retorno'.

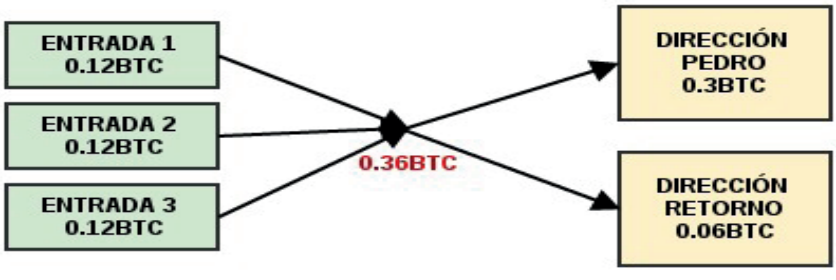
En efecto, las "entradas" representan sumas de bitcoins recibidas en transacciones anteriores y conforman la base de toda transferencia futura, ya que solo se va a poder enviar montos integrados por una o más de ellas. De esta manera, si uno quiere enviar un monto determinado desde una dirección "A" hacia una dirección "B", deberá tomar todas aquellas "entradas" que le permitan poder alcanzar esa suma deseada; y si ello genera un sobrante, toda vez que el monto tomado supera a

aquel que se desea transferir, deberá incluir en la transacción una dirección de retorno (puede ser la misma que la de envío) en la cual recibirlo. De lo contrario, esa suma irá a parar, a modo de "recompensa", a manos de los "mineros" que validaron la transacción.

Continuemos con el ejemplo anterior. Imaginemos que de los 5 bitcoins recibidos en la dirección "A", uno desea conservar en ella la suma de 3.2 y enviar el resto (1.8 bitcoins) hacia la dirección "B". Como los 5 bitcoins fueron recibidos en una única transacción, conforman lo que antes denominamos una "entrada"; por ende, técnicamente, mi transacción siguiente deberá componerse del mismo valor. En ese caso, al concretar la transferencia de 1.8 bitcoins hacia la dirección "B", deberé precisar en mi 'billetera' cuál es la "dirección de retorno" en la que quiero que vuelva ese sobrante de 3.2 bitcoins (puede ser la propia dirección de envío o cualquier otra que uno maneje).

Lo mismo sucede si uno, para enviar la suma deseada, necesita tomar bitcoins de más de una dirección dentro de su propia cartera; no podrá tomar las unidades que quiera, sino aquellas que tengan correlato en una entrada anterior. Por ello, de producirse el mismo sobrante, deberá actuar de idéntica manera y generar la dirección de retorno para no perderlo.

La imagen que se exhibe a continuación representa de manera gráfica lo expuesto anteriormente **(24)**.



Vale remarcar, nuevamente, que la mayoría de las 'billeteras virtuales' están configuradas de forma tal de realizar este proceso en forma sistematizada, sin que el usuario tenga que preocuparse por él. No obstante, es importante conocer cómo se compone el núcleo de una transacción y las distintas variables que puede presentar, ya que, como se verá en los capítulos siguientes, ello tiene una incidencia decisiva en lo que es el funcionamiento de las herramientas que permiten individualizar 'carteras' pertenecientes a las distintas plataformas web que brindan algún tipo de servicio vinculado al Bitcoin, 'llave maestra' para intentar abrir el candado de 'anonimato' en el que operan los usuarios de la red.

Además, su desconocimiento a la hora de analizar la información que brinda sobre una determinada transacción la cadena de bloques (*blockchain*), podría llevarnos a extraer conclusiones equivocadas. En tal sentido, habrá que tener presente que en una transacción en la que se incluya más de una dirección de destino, alguna de ellas puede representar la llamada "dirección de retorno" y haber sido generada por la propia 'billetera' del remitente, lo que implicaría que la suma enlazada en ella no fue transferida, sino que aún continúa en poder de este último.

(24) Para poder alcanzar el monto de 0.3 BTC que se deseaba enviar a la 'dirección' de Pedro, se ha necesitado utilizar tres "entradas" diferentes, cada una por un valor de 0.12 BTC. Dado que entre el monto tomado y la suma a transferir se generó una diferencia de 0.06 BTC, el usuario transferente debió introducir en la transacción una dirección de retorno en la cual recibirlo.

II.3. Búsqueda en la 'cadena de bloques' (blockchain). Información que se puede obtener

Para empezar, es importante destacar que, si bien las transacciones concretadas en la red Bitcoin son totalmente públicas, aquello que revela la 'cadena de bloques' no es más que las direcciones que han participado de cada una de ellas; es decir, permite saber de qué 'dirección bitcoin' hacia qué 'dirección bitcoin' fue transferida una determinada suma de bitcoins, así como también la fecha y la hora de la operación, mas no quién es su "dueño". No brinda ningún dato de identificación de los propietarios y/o administradores de las direcciones que participaron en cada transacción validada.

Tampoco es posible conocer, a través de ella, las direcciones IP de conexión que utilizaron los distintos usuarios de la red para materializar cada una de las transacciones. Aquí hay que recordar que no existe un nodo concentrador o entidad central que regule el funcionamiento del Bitcoin, sino que son los propios operadores quienes, a modo de 'pares' o 'iguales', procesan y transmiten bajo la forma de propagación las transacciones efectuadas, lo que torna extremadamente difícil llegar a obtener esa información.

Ello no significa que, por consiguiente, toda operación con bitcoins quede sepultada en el anonimato, sino que, simplemente, obliga a emplear otros medios para poder individualizar a la persona que está detrás del manejo de una determinada dirección.

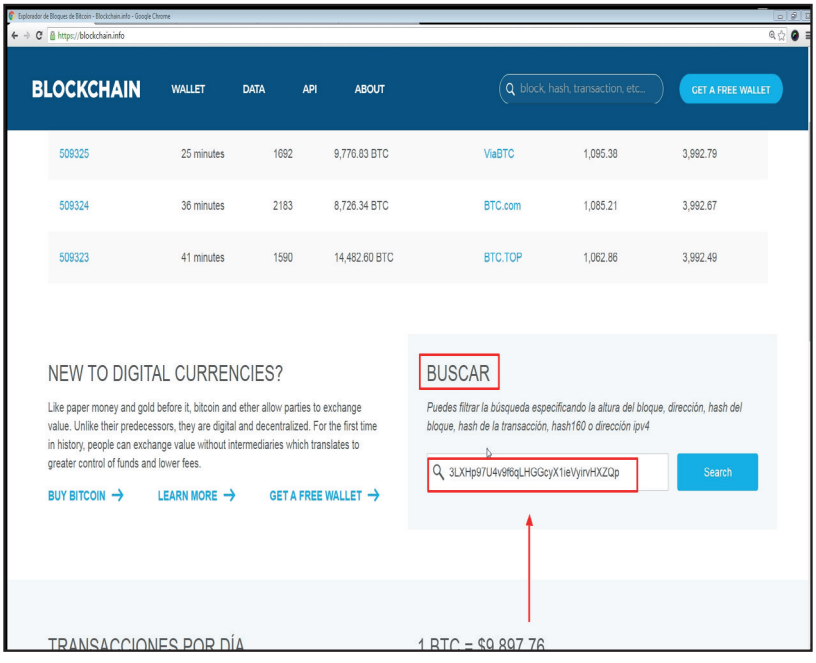
Hay muchos sitios web que ofrecen de manera gratuita el servicio de visualización de la 'cadena de bloques'. Estos se diferencian tanto por el tipo de interfaz gráfica que le brindan al usuario para operar en su plataforma como por la información que presentan —en algunos, se incluyen datos más técnicos; en otros, se evitan en pos de priorizar una interacción más amigable—. La manera de buscar en ellos es sumamente sencilla, aunque es importante conocer de antemano qué información nos interesa obtener. Por ejemplo, si lo que queremos es conocer y analizar todas las transacciones en las que participó históricamente una 'dirección bitcoin' y el saldo que mantiene en la actualidad, será cuestión de enfocar la actividad de búsqueda en esa línea. Por el contrario, si estamos siguiendo una transferencia puntual y queremos saber qué sucedió después, esto es, reconstruir el "árbol" de transacciones generado a partir de ella, conocer por qué montos se materializó cada una y qué direcciones se vieron involucradas —si es que ocurrió ello, ya que tranquilamente la suma transferida pudo haber quedado "congelada" en la dirección inicial que lo recibió—, habrá que dirigirla hacia ese camino. Puede ser, igualmente, que en el marco de nuestra labor nos encontremos frente a un caso en el que nos interese conocer ambas cosas.

Intentemos trabajar con un ejemplo concreto. Veamos cómo se realiza una búsqueda a través de la web *www.blockchain.info* **(25)**. Esta puede iniciarse de dos maneras: consultando los movimientos y el balance que presenta en la cadena de bloques una dirección puntual, o bien preguntando, directamente, por una transacción en particular **(26)**. Para hacer esto último, es necesario conocer, de antemano, el *hash* con que aquella se identifica (es un código que se compone con más de 50 caracteres y actúa como identificador único de cada transacción).

La imagen que se exhibe a continuación refleja el escenario que se nos presenta al acceder a la mencionada web. Dentro de la página principal hay una solapa que se identifica con la palabra "BUSCAR". Allí deben colocarse los caracteres que conforman la dirección que nos interesa consultar o bien, como se dijo, el *hash* que identifica la transacción.

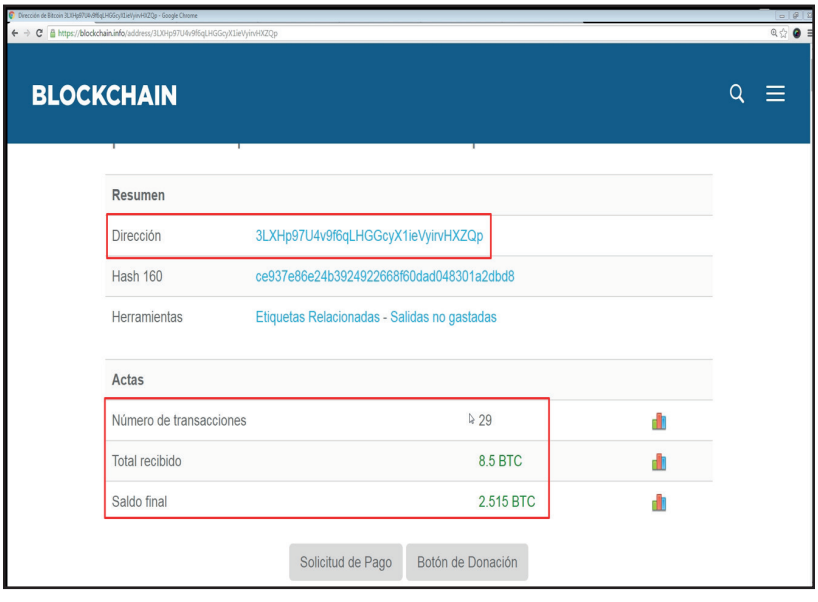
(25) Dicho sitio web es uno más entre tantos otros que ofrecen el servicio de visualización de la cadena de bloques, como por ejemplo https://blockexplorer.com o https://live.blockcypher.com. Su elección para trabajar como ejemplo se debió, simplemente, a que en mi consideración es la que presenta una interfaz gráfica más amigable para el usuario.

(26) También se puede consultar por un determinado bloque añadido a la red y ver los datos técnicos detrás de su composición, incluidas las transacciones que lo integran. Sin embargo, dada la finalidad de este trabajo, carece de sentido profundizar la explicación sobre esta modalidad de búsqueda.



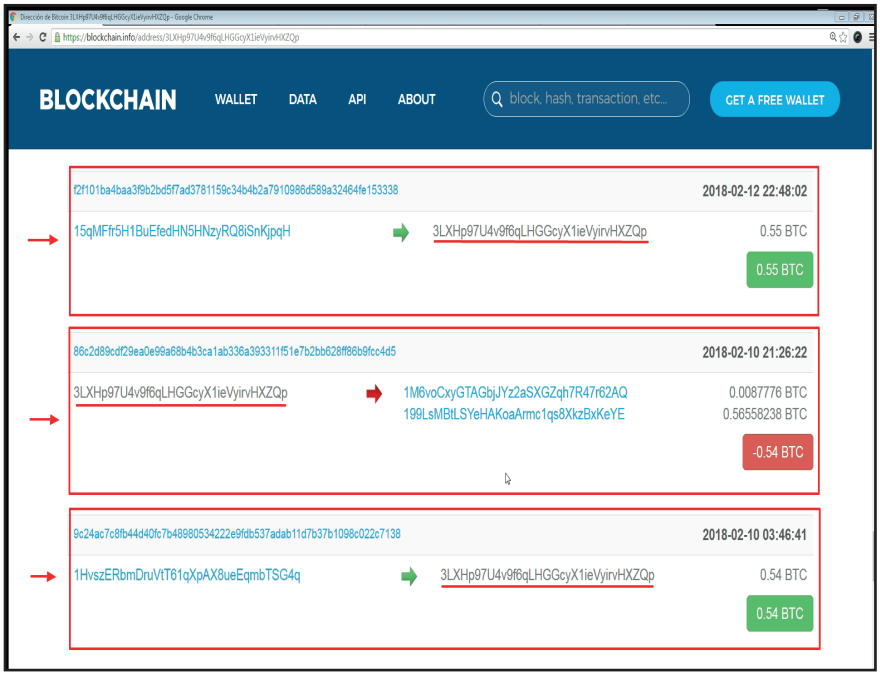
www.blockchain.info

La consulta sobre una dirección en particular arroja como resultado, en primer lugar, un balance inicial de ella: número de transacciones en las que participó, total de bitcoins que recibió y saldo actual, esto es, unidades que aún mantiene enlazadas.



https://blockchain.info/es/address/3LXHp97U4v9f6qLHGGcyX1ieVyirvHXZQp

En segundo término, brinda un listado ordenado en forma cronológica con todas las operaciones en que participó, el cual incluye tanto transferencias recibidas como realizadas. Sobre cada una de ellas, además, se especifica la fecha y la hora en que tuvo lugar, el *hash* con el que se identifica, el monto por el cual se concretó (detallándose la suma que envió o recibió) y la o las direcciones con las que operó.

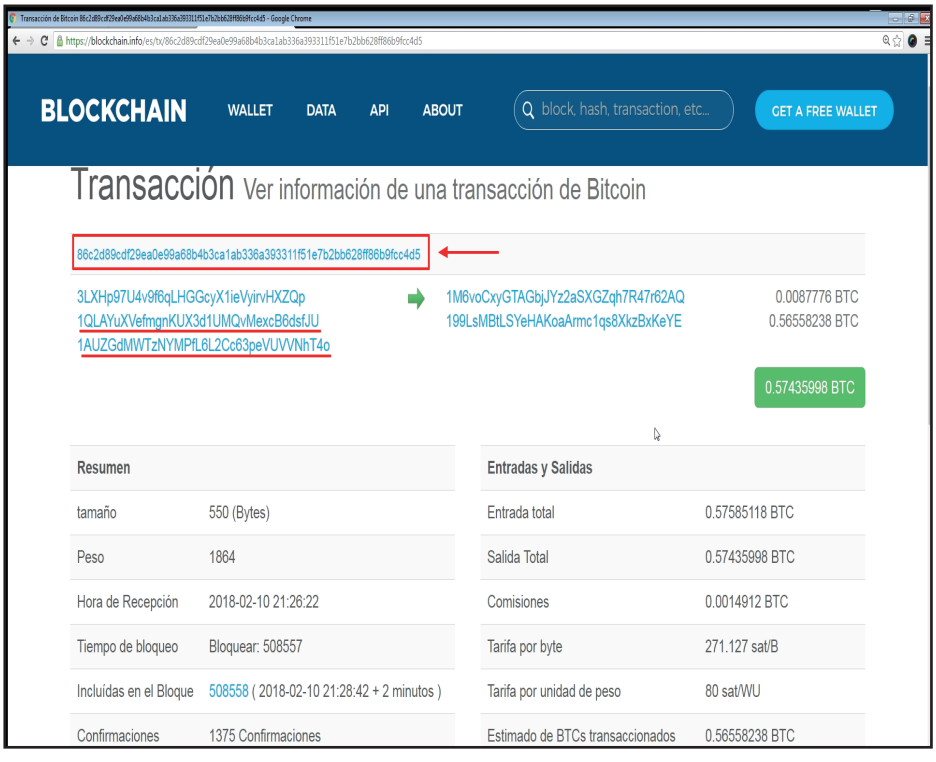


https://blockchain.info/es/address/3LXHp97U4v9f6qLHGGcyX1ieVyirvHXZQp

Sin embargo, el listado se enfoca exclusivamente en la dirección consultada y por ello no ofrece el detalle completo de la transacción; es decir, si hubo alguna otra dirección que envió sumas de bitcoins junto a ella, no aparece. Tampoco, en el caso opuesto, si hubo alguna otra que recibió a su par. Por tal motivo, si se desea ver esa información, será necesario *cliquear* sobre el *hash* que identifica la transacción.

La siguiente imagen corresponde al detalle de la transacción que luce en la segunda posición del listado antes exhibido. En ella se puede advertir claramente cómo se incorporan dos nuevas direcciones dentro del grupo remitente **(27)**.

(27) Hay que tener en cuenta que en esta plataforma, al brindarse el detalle de una transacción, no se especifican las entradas que la conforman. Por ello, de haber más de una dirección remitente, tampoco se indica la suma de bitcoins que ha enviado cada una. Igualmente, de resultar de interés, ese dato puede conocerse de manera muy sencilla. Simplemente habrá que clickear sobre cada dirección, localizar la transacción en el listado de operaciones —la cual va a estar enfocada desde su aporte— y verificarlo; o en su defecto, consultar directamente la transacción (a partir del hash único que lo identifica) en algún otro sitio que brinde el servicio de visualización de la cadena de bloques e incluya esa información en particular, como pueden ser, por ejemplo, https://live.blockcypher.com o www.blocktrail.com.



https://blockchain.info/es/tx/86c2d89cdf29ea0e99a68b4b3ca1ab336a393311f51e7b2bb628ff86b9fcc4d5

Para consultar por una transacción puntual, será necesario conocer, como se dijo, el *hash* único que identifica la transacción: sin embargo, difícilmente ese dato esté a nuestro alcance al momento de iniciarse una búsqueda. En este sentido, lo más probable es que, cuando estemos frente a una investigación en la que nos interese seguir una transferencia concreta, sepamos únicamente el monto y la fecha de la operación, la dirección en que se recibió y, a lo sumo, aquella desde la cual se envió. En ese caso, lo más fácil será efectuar directamente la consulta sobre aquella dirección que actuó como receptora del pago; y una vez que la búsqueda nos arroje todas las operaciones en las que participó históricamente, localizar con los datos antes destacados la transacción en particular que es de nuestro interés. A partir de allí, podremos comenzar el trabajo de indagación.

La metodología para reconstruir el árbol y ver las operaciones que la sucedieron, no presenta ningún tipo de dificultad. Será cuestión de ir *clickeando* sobre cada dirección que actúa como receptora y ver en el listado cronológico de sus transacciones si con posterioridad a recibir el respectivo monto materializó alguna transferencia y, en su caso, por qué valor. Habrá que tener presente, conforme se explicó, que la suma que reciba una dirección se integra a los fondos ya enlazados en ella y, por ende, puede formar parte de una transacción siguiente por un monto mayor.

II.4. Herramientas informáticas de identificación de 'billeteras virtuales'

En la actualidad, varias empresas han desarrollado herramientas que permiten, por medio de la utilización de algoritmos y a partir de un análisis profundo de las transacciones validadas en la red, entre otras técnicas empleadas, identificar las distintas direcciones que componen una misma 'bi-

lletera' y, más importante aún, determinar cuáles de ellas pertenecen a las plataformas web más destacadas dentro del ecosistema Bitcoin.

Básicamente lo que hacen es estudiar las distintas 'direcciones bitcoin' involucradas en cada operación y, en función de determinados comportamientos evidenciados, agruparlas como posibles integrantes de una misma 'cartera'. A la par, dicha información es complementada con aquella obtenida de una interacción constante con las plataformas mencionadas, la cual surge de realizar depósitos y retiros de sumas de bitcoins en forma continua **(28)**, de forma tal de poder hacer un trabajo asociativo que les permita vincularlas.

Ahora bien, ¿de qué nos sirve en una investigación contar con la información que pueden brindar estas herramientas de identificación? Sin lugar a duda, es de gran utilidad. Tratemos de analizarlo a partir de un ejemplo concreto. Imaginemos que estamos trabajando en un caso en el que se investiga una extorsión en la que su autor —una persona no individualizada— exige a la víctima un pago en bitcoins; y para ello, le brinda una 'dirección bitcoin' en la cual materializar la transferencia. Si realizáramos una búsqueda en la 'cadena de bloques', tal como explicamos antes, a lo sumo podríamos saber si esa dirección participó en alguna transacción y, en su caso, cuándo tuvo lugar y por qué monto. No más que eso. No tendríamos manera de avanzar en la identificación del extorsionador. Al menos, no por esta vía.

Precisamente, el uso de estas herramientas lo que nos permitiría conocer, a partir del trabajo asociativo que hacen, es si la dirección involucrada integra, junto a alguna otra, una misma 'billetera'; y más relevante aún, si alguna de ellas, en alguna oportunidad, concretó una transferencia de bitcoins hacia una dirección administrada por una de estas plataformas web que presta algún tipo de servicio vinculado al Bitcoin. De ser así, claramente abriríamos una puerta para lograr la identificación de la persona que está detrás del acto extorsivo que investigamos. Sin embargo, para profundizar esta línea de indagación sin cometer errores, necesitaríamos saber, primero, el significado de esa transacción. ¿Qué representó esa transferencia de bitcoins hacia dicha plataforma? ¿Una mera operación de compra/venta entre dos usuarios de la red? ¿El pago de un servicio o la compra de un producto? ¿Un mero traspaso de fondos por parte del mismo individuo?

Para responder ello, es imprescindible conocer qué servicio presta la respectiva plataforma. Por ejemplo, si lo que hace es brindarles a distintos sitios web o locales comerciales un sistema de procesamiento para que puedan aceptar pagos en bitcoins sin tener que preocuparse en administrar y resguardar las direcciones en las que los reciben (como ofrecen los sitios BitPay.com u OkPay.com), sabremos que la transferencia en cuestión debió significar, probablemente, una compra en alguno de estos lugares. Será cuestión que desde la propia plataforma nos indiquen a qué empresa se le asignó el pago, para tomar contacto con un representante de ella y obtener los datos de identificación del cliente que lo realizó, información que, indudablemente, nos acercaría mucho a la persona que está detrás de la extorsión investigada.

En cambio, si la plataforma lo que hace es prestar el servicio de custodia y manejo de fondos ('billetera online'), podríamos estar ante dos escenarios distintos: un posible traspaso de fondos concretado por el mismo individuo, de una cartera a otra; o una transacción que realizó con otra persona. Sea cual sea el caso, a partir de la información que brinde la plataforma, podremos individualizar a quien recibió la transferencia de bitcoins; y desde allí, comenzar a trabajar en miras a desentrañar si se trata del propio autor del hecho o, en su defecto, de alguien vinculado a él.

Así, podríamos seguir con muchos más ejemplos. La escena que nos presentaría una plataforma que, además, funciona como *exchange* (casa de cambio online) u ofrece herramientas de *trading* (ventas o compras programadas, negociación de 'futuros'), podría ser totalmente distinta. Lo mismo con aquella que opera como vía de pago a nivel global, como si fuese una especie de banco virtual; o la que se dedica, simplemente, a conectar vendedores y compradores, actuando como 'garante' de la transacción. En definitiva, cada servicio que pueden prestar estas platafor-

(28) Esta acción permite conocer cómo administran y resguardan los fondos que manejan, además de revelar algunas de las direcciones que componen sus monederos principales —tanto los que utilizan diariamente como aquellos que "congelan" con grandes sumas enlazadas—.

mas nos obliga a pensar situaciones diferentes y a tomar los recaudos necesarios para evitar caer en interpretaciones equivocadas que nos lleven, procesalmente hablando, a tomar decisiones erróneas que impacten negativamente en el curso de una investigación. De allí la importancia de estudiarlas en profundidad y poder asignarle el significado correcto a la operación examinada.

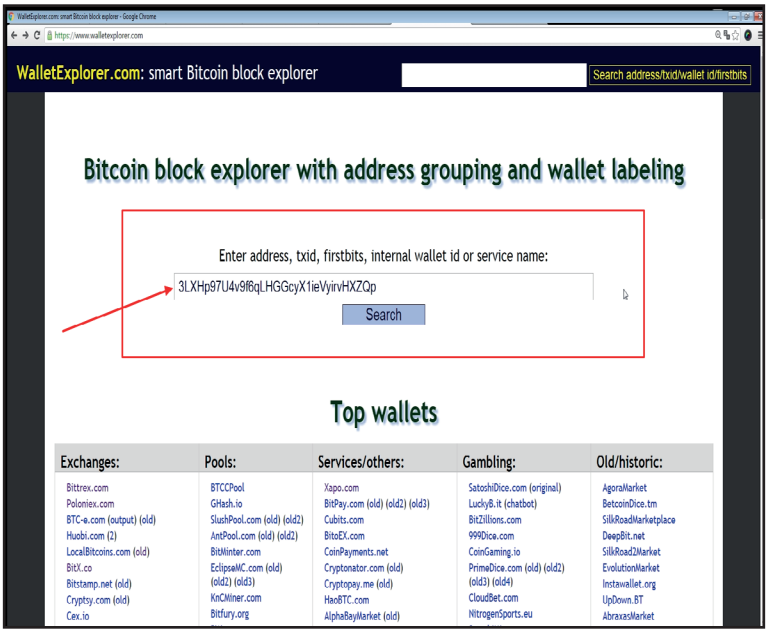
Hasta aquí, no quedan dudas de lo útil que pueden ser estas herramientas de identificación. No solo para individualizar a quien podría detrás del manejo de una cartera, sino también para rastrear, localizar y eventualmente congelar fondos de origen ilícito, ya que, de determinarse su almacenamiento y resguardo en alguna de estas plataformas, será cuestión de recurrir a la empresa que la administra para que materialice su aseguramiento.

Como señalé anteriormente, se trata de herramientas comercializadas por empresas que se dedican a ofrecer soluciones en análisis y búsqueda de datos en blockchain. Sus principales clientes son instituciones financieras, agencias de gobierno y las propias compañías —serias— que brindan servicios vinculados al Bitcoin y no tienen interés alguno en que fondos criminales se almacenen en sus cuentas. La más conocida del mercado es Chainalysis Inc. (www.chainalysis.com).

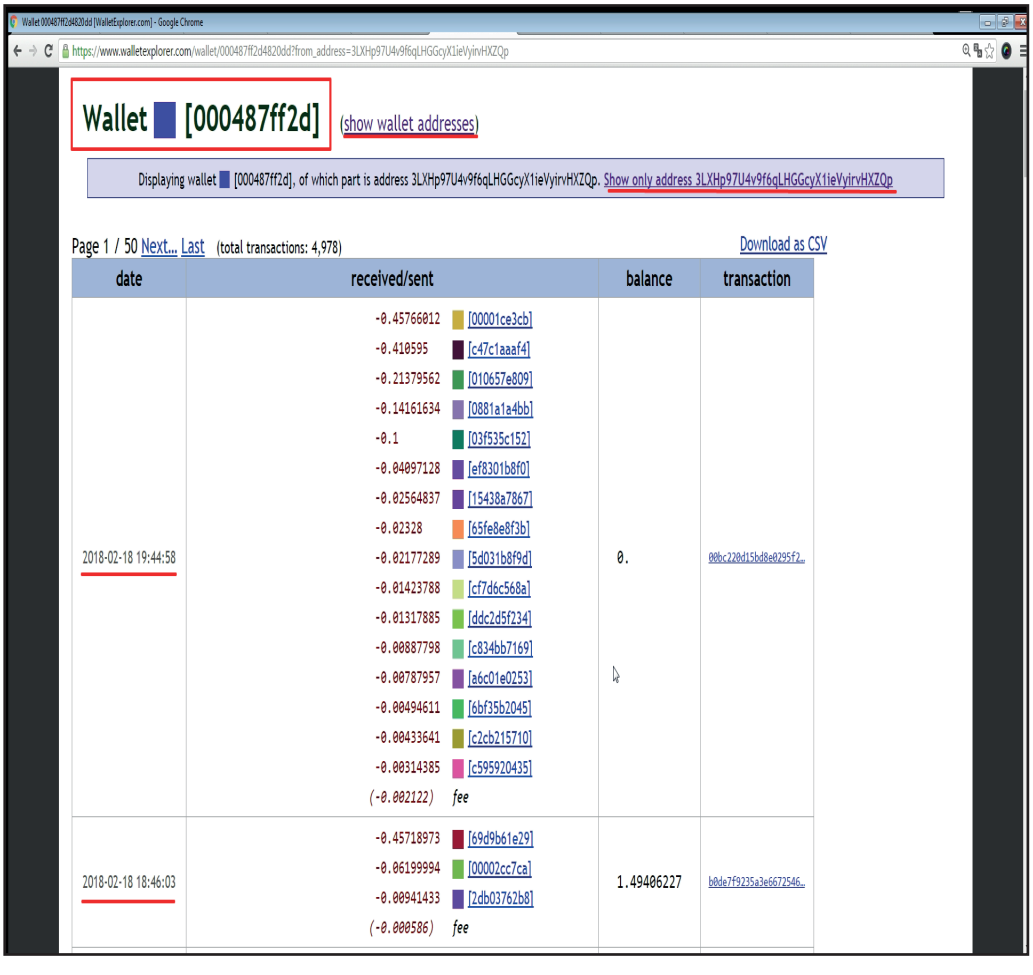
En la propia web se puede encontrar un sitio (www.WalletExplorer.com) que brinda, de manera gratuita, una versión online de esta herramienta, aunque menos sofisticada y, obviamente, con menos información y recursos disponibles, ya que no tiene el grado de actualización permanente que evidencian aquellas que son comercializadas. Sin embargo, su uso en una investigación puede, eventualmente, ser igual de valioso, por lo que intentaré mostrar, aunque sea mínimamente, cómo se opera a través de ella, y así cerrar con un ejemplo visual la explicación sobre la metodología de trabajo propuesta.

El inicio de búsqueda es igual que en cualquier página que permita la visualización de la cadena de bloques. Puede consultarse por una dirección puntual o bien por una transacción concreta (por medio del respectivo *hash* que la identifica).

Veamos qué sucede en el primer caso. La imagen exhibida a continuación refleja una consulta sobre la misma dirección con la que antes veníamos trabajando.



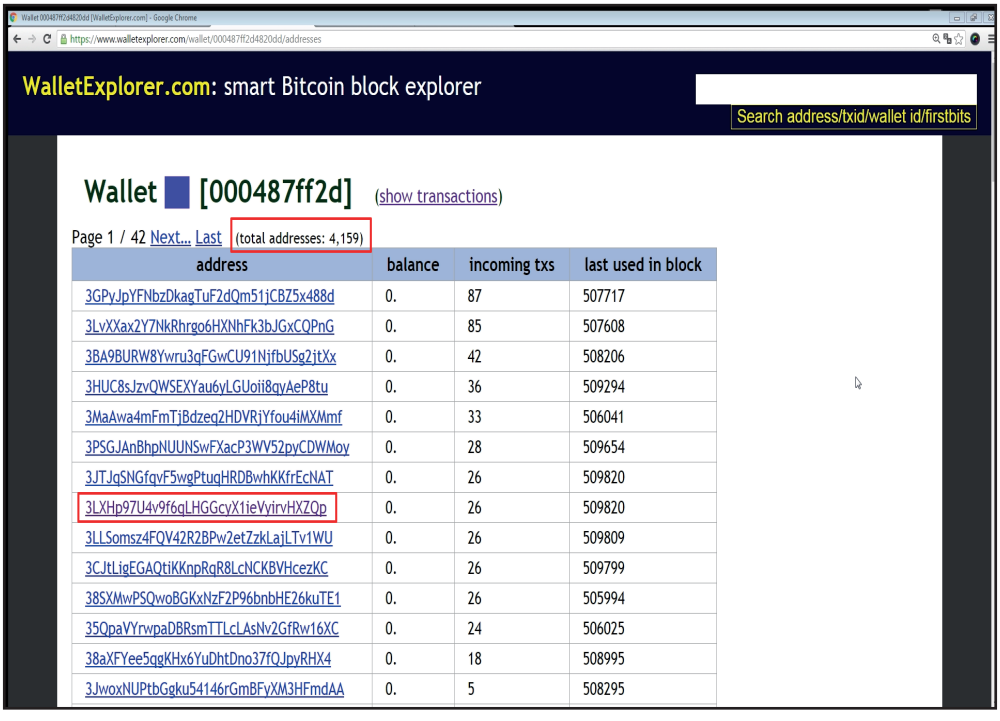
Como respuesta, la página nos va a arrojar un listado de operaciones ordenado en forma cronológica que no pertenece únicamente a la dirección Bitcoin consultada, sino a todas las direcciones que la herramienta, a partir del uso de un algoritmo específico y bajo los lineamientos que ya se explicó, estima que integran una misma 'billetera virtual', a la cual, además, identifica con un código compuesto por diez caracteres alfanuméricos al solo efecto de facilitar la lectura e interpretación de la información que brinda **(29)**.



Los destinatarios de esas operaciones son identificados por la herramienta de igual manera; como 'billeteras' que pueden ser integradas por una o más direcciones. En la propia imagen puede observarse, a su vez, como el sitio le ofrece al usuario verificar tanto las direcciones que componen esta supuesta billetera (recordar que no deja de ser una estimación, aunque con gran probabilidad de acierto por la base científica en que se apoya) como las transacciones exclusivas que involucran a la dirección que fue objeto de consulta.

(29) La identificación de esta billetera bajo esos caracteres es una creación propia de la web, completamente ajena a la red Bitcoin.

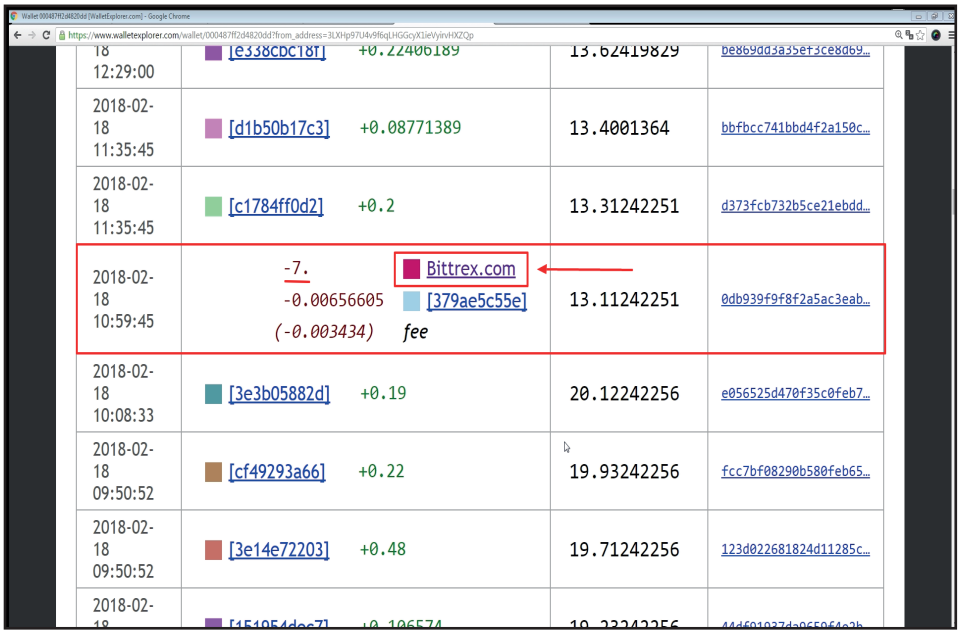
La siguiente imagen exhibe, precisamente, el listado con la totalidad de direcciones que la herramienta asocia a esta misma cartera.



address	balance	incoming txs	last used in block
3GPyJpYFNbzDkagTuF2dQm51jCBZ5x488d	0.	87	507717
3LvXXax2Y7NkRhrgo6HXNhFk3bJGxCQPnG	0.	85	507608
3BA9BURW8Ywru3qFGwCU91NjfbUSg2jtXx	0.	42	508206
3HUC8sJzvQW5EXYau6yLGUoii8qvAeP8tu	0.	36	509294
3MaAwa4mFmTjBdzeq2HDVRjYfou4iMXMmf	0.	33	506041
3PSGJAnBhpNUUNSwFXacP3WV52pyCDWMoy	0.	28	509654
3JTJqSNGfqvF5wgPtuqHRDBwhKKfrEcNAT	0.	26	509820
3LXHp97U4v9f6qLHGGcyX1ieVyirvHXZQp	0.	26	509820
3LLSomsz4FQV42R2BPw2etZzkLajLTv1WU	0.	26	509809
3CJtLigEGAQtiKKnpRqR8LcNCKBVHcezKC	0.	26	509799
38SXMwPSQwoBGKxNzF2P96bnbHE26kuTE1	0.	26	505994
35QpaVYrwpaDBRsmTTLcLAsNv2GfRw16XC	0.	24	506025
38aXFYee5qgKHx6YuDhtDno37fQJpyRHX4	0.	18	508995
3JwoxNUPtbGgku54146rGmBFyXM3HFmdAA	0.	5	508295

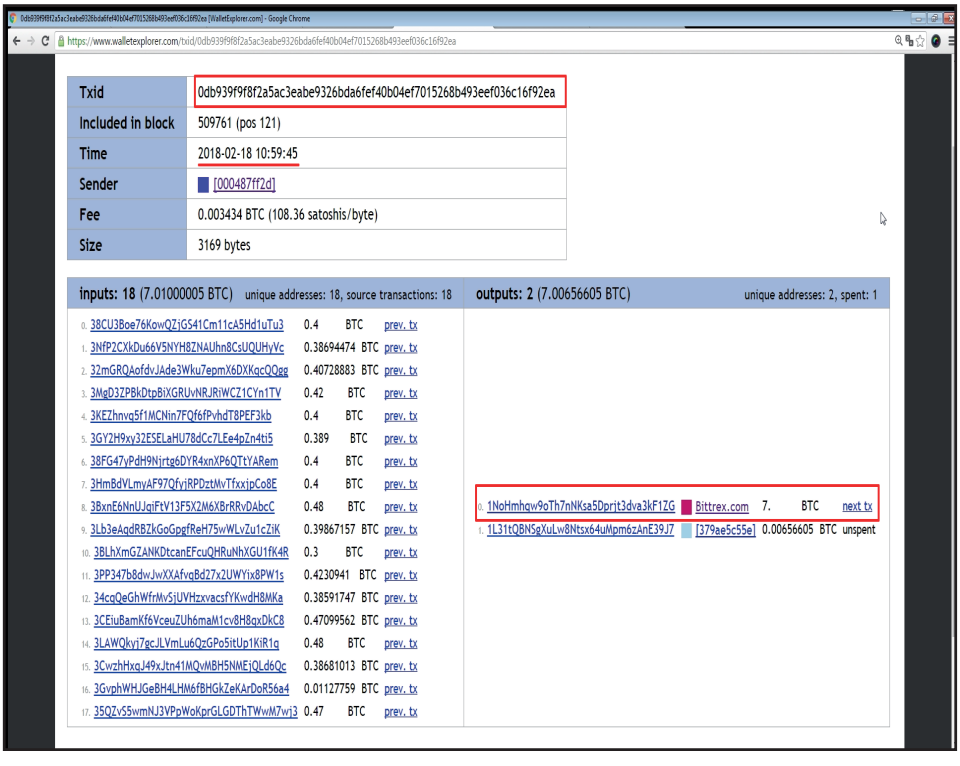
Ahora bien, conforme ya se explicó, la llave para identificar a quién está detrás del manejo de una determinada 'dirección bitcoin', consiste en estudiar los movimientos que presenta la 'billetera que integra' (es decir, todas las direcciones asociadas a ella) y verificar si, en algún momento, concretó una transferencia hacia alguna 'cartera' perteneciente a una plataforma web a la cual, eventualmente, se le pueda requerir información sobre el usuario involucrado.

En el caso que venimos trabajando como ejemplo, se advirtieron varias transacciones concretadas hacia direcciones administradas por plataformas conocidas. La imagen que se exhibe a continuación refleja, precisamente, una transferencia efectuada hacia una billetera que pertenecería a la plataforma administrada por la compañía Bittrex (www.bittrex.com), la cual ofrece, como principal servicio, la compraventa de distintas cripto-monedas (actividad conocida internacionalmente como *exchange*).



12:29:00	[e338cdc18f]	+0.22406189	13.62419829
2018-02-18 11:35:45	[d1b50b17c3]	+0.08771389	13.4001364
2018-02-18 11:35:45	[c1784ff0d2]	+0.2	13.31242251
2018-02-18 10:59:45	-7. -0.00656605 (-0.003434)	Bittrex.com [379ae5c55e] *fee*	13.11242251
2018-02-18 10:08:33	[3e3b05882d]	+0.19	20.12242256
2018-02-18 09:50:52	[cf49293a66]	+0.22	19.93242256
2018-02-18 09:50:52	[3e14e72203]	+0.48	19.71242256
2018-02-	[151954dec7]	+0.106574	19.33242256

Para ver el detalle de la transacción (direcciones involucradas, montos enviados por cada una), simplemente hay que *clickear* en el *hash* que la identifica.



Txid	0db939f9f8f2a5ac3eabe9326bda6fef40b04ef7015268b493eef036c16f92ea
Included in block	509761 (pos 121)
Time	2018-02-18 10:59:45
Sender	[000487ff2d]
Fee	0.003434 BTC (108.36 satoshis/byte)
Size	3169 bytes

inputs: 18 (7.01000005 BTC) unique addresses: 18, source transactions: 18

0.	38CU3Boe76KowQZjGS41Cm11cA5Hd1uTu3	0.4 BTC	prev. tx
1.	3NfP2CXkDu66V5NYH8ZNAUhn8CsUQUHyVc	0.38694474 BTC	prev. tx
2.	32mGRQAofdvJAde3Wku7epmX6DXKqcQQgg	0.40728883 BTC	prev. tx
3.	3MgD3ZPBkDtpBiXGRUvNRJRiWCZ1CYn1TV	0.42 BTC	prev. tx
4.	3KEZhnvq5f1MCNin7FQf6fPvhdT8PEF3kb	0.4 BTC	prev. tx
5.	3GY2H9xy32E5ELaHU78dCc7LEe4pZn4ti5	0.389 BTC	prev. tx
6.	38FG47yPdH9Njrtg6DYR4xnXP6QTtYARem	0.4 BTC	prev. tx
7.	3HmBdVLmyAF97QfyjRPDztMvTfxxjpCo8E	0.4 BTC	prev. tx
8.	3BxnE6NnUJqiFtV13F5X2M6XBrRRvDAbcC	0.48 BTC	prev. tx
9.	3Lb3eAqdRBZkGoGpgfReH75wWLvZu1cZiK	0.39867157 BTC	prev. tx
10.	3BLhXmGZANKDtcanEFcuQHRuNhXGU1fK4R	0.3 BTC	prev. tx
11.	3PP347b8dwJwXXAfvqBd27x2UWYix8PW1s	0.4230941 BTC	prev. tx
12.	34cqQeGhWfrMvSjUVHzxvacsfYKwdH8MKa	0.38591747 BTC	prev. tx
13.	3CEiuBamKf6VceuZUh6maM1cv8H8qxDkC8	0.47099562 BTC	prev. tx
14.	3LAWQkyj7gcJLVmLu6QzGPo5itUp1KiR1q	0.48 BTC	prev. tx
15.	3CwzhHxqJ49xJtn41MQvMBH5NMEjQLd6Qc	0.38681013 BTC	prev. tx
16.	3GvphWHJGeBH4LHM6fBHGkZeKArDoR56a4	0.01127759 BTC	prev. tx
17.	35QZv55wmNJ3VPpWoKprGLGDThTWvM7wj3	0.47 BTC	prev. tx

outputs: 2 (7.00656605 BTC) unique addresses: 2, spent: 1

0.	1NoHmhqw9oTh7nNKsa5Dprjt3dva3kF1ZG	Bittrex.com	7. BTC	next tx
1.	1L31tQBN5gXuLw8Ntsx64uMpm6zAnE39J7	[379ae5c55e]	0.00656605 BTC	unspent

De allí en más, comenzará el trabajo ya explicado de interpretar qué representa la transacción, a partir del servicio que presta la plataforma, y contactar a la empresa que la administra para que nos brinde la información del usuario al que se le acreditaron los fondos enviados.

II.5. Descripción de las principales plataformas que prestan algún tipo de servicio vinculado al bitcoin

La importancia de conocer qué servicio brindan las distintas plataformas del ecosistema Bitcoin ya ha sido señalada en varias oportunidades a lo largo de este trabajo. Sin embargo, abordar una explicación de todas y cada una de ellas, resultaría una tarea de muy difícil concreción, máxime teniendo en cuenta que, a raíz de la expansión que ha evidenciado el uso de esta cripto-moneda a nivel mundial en los últimos años, se ha multiplicado la aparición de nuevos desarrollos comerciales. Por ende, el foco de este capítulo va a estar centrado en describir únicamente el funcionamiento de las más conocidas y utilizadas (que más volumen de mercado abarcan) a escala global, las cuales, en definitiva, ofrecen la mayoría de los servicios hoy disponibles.

También se hará una mínima mención sobre cómo operan las plataformas conocidas bajo el nombre de "Mixer" (mezcladora) y qué dificultades nos pueden traer en el marco de una investigación a la hora de intentar reconstruir un flujo de fondos.

II.5.a. LocalBitcoins (www.localbitcoins.com)

Se trata de una plataforma virtual (a la que se puede acceder tanto vía web como a través de una aplicación móvil) que tiene como objeto, a partir de la interacción entre sus usuarios y por medio de la publicación de anuncios, permitir la compraventa de bitcoins, con la particularidad de que el sitio actúa como intermediario en cada transacción.

La manera de operar dentro de ella es la siguiente: aquel usuario que desee ofrecer la venta de bitcoins, deberá tener almacenada la respectiva cantidad ofertada en su propia 'billetera virtual'. Una vez que el eventual comprador, también usuario de la plataforma, se muestra interesado en la oferta e inicia el proceso de adquisición de la suma de bitcoins —el cual incluye una interacción con el vendedor a fin de cerrar los aspectos formales de la operación—, el monto ofrecido es extraído automáticamente de la cuenta del vendedor y alojado en un depósito de garantía administrado por el sitio. Concretado el pago y confirmada su recepción por el vendedor, se libera el monto de bitcoins retenidos y se deposita en una de las direcciones que integran la billetera del comprador.

Para operar en la plataforma se debe estar previamente registrado (se debe superar un proceso de identificación —Know Your Customer—). La empresa que la administra es LocalBitcoins Oy y, según se indica en el propio sitio web, tiene sus oficinas en la ciudad de Helsinki, Finlandia, y se halla inscripta tanto en el registro mercantil como en el organismo de control de entidades financieras de dicho país.

II.5.b. Bitpay (www.bitpay.com)

Esta plataforma (a la que también se puede acceder por medio de una aplicación móvil) se dedica a prestar una gran variedad de servicios vinculados al Bitcoin, tanto a nivel empresarial como individual. Se destaca, principalmente, por ser reconocida mundialmente como la mayor procesadora de pagos del mercado. Ese es el principal servicio que presta y el que utiliza la mayoría de sus clientes. Consiste en ofrecer tanto a los sitios web como a locales comerciales, la posibilidad de adherir el Bitcoin como opción de pago.

A la par de ello, también brinda carteras para que sus usuarios puedan operar individualmente en la red o realizar pagos en comercios adheridos. Incluso hasta ofrece la opción de obtener tarjetas de débito para utilizar en distintos países del mundo, respaldadas con sumas de bitcoins depositadas en cuentas abiertas dentro de la propia plataforma.

La empresa que administra la web es Bitpay Inc. y sus oficinas se ubican en la ciudad de Atlanta, Georgia (Estados Unidos de América). Según se indica en el propio sitio web, se encuentra sujeta a las leyes y regulaciones de dicho país.

II.5.c. Binance (www.binance.com)

Se trata de la plataforma más utilizada en la actualidad a nivel mundial. Es la que más visitas semanales promedio presenta y más operaciones de intercambio realiza **(30)**. Se destaca por prestar una gran variedad de servicios vinculados tanto al Bitcoin como a otras criptomonedas (incluso variedad de tokens monetizados, que responden a protocolos DeFi —Finanzas Descentralizadas—), además de permitir operar con una gran cantidad de monedas fiduciarias de distintos países. Al igual que las anteriores, también se puede acceder a ella por medio de una aplicación móvil.

Para empezar, ofrece a los usuarios el servicio de 'billetera online', a través del cual pueden recibir y enviar fácilmente sumas de bitcoins, como así también de otras 'monedas virtuales'. En línea con ello, brinda un espacio para su compraventa, para lo cual actúa como si fuese una casa de cambio común y corriente, pero que opera de manera virtual: uno puede tanto depositar en su cuenta sumas de bitcoins que estén en su poder y retirar su valor en moneda fiduciaria, como realizar el procedimiento opuesto: depositar o transferir sumas de esta última, comprar bitcoins y retirarlos, es decir, transferirlos a alguna otra billetera virtual ajena al sitio (también está la posibilidad de intercambiarlo por alguna otra cripto-moneda). Las opciones de pago y retiro de dinero dependerán, básicamente, del lugar desde el cual uno opere. No obstante, para superar cualquier eventual restricción, brinda un espacio de compraventa entre usuarios denominado P2P, el cual permite que entre ellos acuerden los términos de la transacción y concreten el intercambio de manera presencial —pago en efectivo—, limitándose la plataforma a actuar como 'garante' de la operación.

Dentro de la plataforma también es posible realizar diversas operaciones de *trading*, como programar órdenes de compra y de venta a futuro, sujetas a determinadas condiciones; u obtener una tarjeta de débito para utilizar en distintos países del mundo, respaldada, precisamente, con sumas de bitcoin (u otra cripto-monedas) almacenadas en ella. Por su parte, a nivel empresarial, también actúa como procesador de pagos y ofrece tanto a los sitios web como a locales comerciales, la posibilidad de adherir el Bitcoin dentro de sus opciones de cobro.

En cuanto a la ubicación física de sus oficinas o sede legal, no es posible dar una respuesta precisa. Como lo marcan infinidad de notas periodísticas publicadas por sitios especializados, Binance opera como un 'negocio descentralizado' a través del cual buscaría escapar, al menos por el momento, a toda regulación local sobre sus actividades. De allí la imposibilidad de situarla sobre una jurisdicción en particular.

II.5.d. CoinBase (www.coinbase.com)

Esta plataforma cuenta como servicio principal el ofrecer a los usuarios una cuenta a través de la cual poder recibir, almacenar y enviar fácilmente tanto sumas de bitcoins como de otras cripto-monedas (entre ellas, Ether, Litecoin, BitcoinCash, XRP). Al igual que las anteriores, brinda la posibilidad de asociar a dicha cartera una tarjeta de débito para utilizar de manera física en locales comerciales y/o retirar dinero en efectivo de cajeros automáticos. También ofrece un espacio para que los usuarios puedan realizar diversas operaciones de *trading* (órdenes de compra bajo ciertas condiciones, compras a futuro, etc.). Asimismo, a nivel empresarial, se destaca por prestar un sistema de procesamiento de pagos que permita tanto a sitios web como a locales comerciales aceptar cripto-monedas dentro de sus opciones de cobro.

Sin embargo, el servicio más novedoso que brinda lo constituye el otorgamiento de préstamos dinerarios con respaldo en sumas de bitcoins almacenadas en la plataforma. Según se explica en la propia web, el atractivo de la propuesta consiste en permitirle a aquel usuario que esté necesitado de conseguir dinero líquido en forma urgente, la posibilidad de evitar tener que desprenderse de las unidades de valor de dicha cripto-moneda, lo que podría significarle un mal negocio, atendiendo a las constantes fluctuaciones de precio que suele evidenciar.

La empresa principal que administra la plataforma es “Coinbase Inc.” y se encuentra radicada en la ciudad de San Francisco, California, Estados Unidos de América.

(30) www.coinmarketcap.com/es/rankings/exchanges.

II.5.3. Xapo (www.xapo.com)

Esta plataforma se destaca por ofrecer a los usuarios un servicio de 'billetera virtual' para usar de manera cotidiana, a través de la cual se pueden recibir, comprar, almacenar y enviar bitcoins fácilmente, con la particularidad de que la compañía se encuentra regulada como banco digital en Gibraltar (autorizada por la GFSC— Gibraltar Financial Services Comission—), lo que le da un parámetro de seguridad diferente. A través de la propia 'cartera' también es posible depositar, transferir o extraer dólares estadounidenses, y asociar a ella una tarjeta de débito para utilizar en una gran cantidad de países del mundo. Es decir, funciona como una cuenta integrada entre sumas de bitcoins y de la mencionada divisa.

Por otra parte, la compañía que administra la plataforma también se destaca por brindar un servicio de custodia de grandes sumas de bitcoins a través de lo que se denomina 'almacenamiento en frío', es decir, fuera de línea. Según se indica en su propia página web, utilizarían una especie de bóveda sumamente protegida, la cual se garantiza que no está expuesta a ningún tipo de injerencia.

La empresa que administra la plataforma es Xapo Holding Limited y, como se mencionó, se encuentra sujeta a las leyes y regulaciones de Gibraltar.

II.5.f. Breve explicación sobre cómo funcionan las plataformas denominadas "mixer"

Dentro del mundo Bitcoin existen varias plataformas que se dedican, específicamente, a brindar un servicio que se conoce con el nombre de "mixer", o como su propia traducción lo indica, "mezclador" **(31)**. En concreto, lo que ellas hacen es intercambiar las unidades de bitcoins que están en posesión de una persona, con los de alguna otra, y así confundir el flujo de fondos, de forma tal de permitir que se pierda el rastro de una operación; es decir, permite romper el seguimiento de una cadena de bloques.

La manera de operar de este tipo de plataformas es muy sencilla. Recibe por parte de los usuarios una determinada suma de bitcoins y les devuelve el mismo monto —restando, obviamente, el cobro de una determinada comisión—, pero distribuido en varias operaciones y utilizando para ello sumas que fueron depositadas por otros usuarios. Así, cruza los saldos y los re-integra de manera 'partida' a través de varias transacciones, tornado prácticamente imposible poder trazar un seguimiento de ellos.

Una de las finalidades buscadas por aquellas personas que utilizan este servicio (mixer) es evitar ser rastreados a partir de la reconstrucción de la cadena de bloques. Por tal motivo, el éxito de los sitios que lo ofrecen radica en operar bajo el anonimato absoluto y que el usuario que se acerque a ellos confíe en que ningún tipo de información suya va a ser revelada en ninguna circunstancia, menos aún, ante un requerimiento judicial.

II.6. Algunas consideraciones sobre la actividad cautelar

Como punto de partida, es importante tener presente que los diferentes modelos de 'billetera virtual' que permiten a un usuario realizar operaciones con bitcoins impactan de lleno en lo que es la tarea de planificación de la actividad cautelar; es decir, la posibilidad concreta de incautar unidades de valor de esta cripto-moneda (en realidad, técnicamente hablando, no sería 'incautar' sino tomar control de esos fondos y disponer de ellos sin que otro —su dueño, por ejemplo— lo pueda hacer) va a depender, básicamente, de que se adopte un curso de acción acorde al escenario particular que presenta cada modalidad de almacenamiento.

Ello es así debido a las marcadas diferencias que exhiben en cuanto a sus características y funcionalidades. Claramente no es lo mismo ser uno responsable de su custodia (ya sea a través de un programa que corre en un dispositivo propio y está conectado a la red Bitcoin, o bien por medio de un dispositivo físico que se mantiene 'congelado' o fuera de línea) que delegar dicha tarea en una empresa que provea tal servicio.

(31) Uno de los más conocidos era BitcoinFog, el cual operaba dentro de lo que se denomina la Deep Web. Según las noticias periodísticas, su fundador fue arrestado el año pasado en el aeropuerto de Los Ángeles, Estados Unidos de América, y actualmente enfrenta cargos criminales ante la justicia de este país por hechos de lavado de activos.

Si bien lo ideal sería desarrollar una línea de trabajo para cada modelo de billetera en particular, dicha labor, por la cantidad de elementos a considerar y la profundidad de análisis requerida, no solo excedería el sentido práctico de este artículo, sino que ameritaría ser abordada en un proyecto de investigación especialmente dedicado a ello. Por tal motivo, me ceñiré simplemente a trazar ciertos lineamientos que, desde mi óptica, deben ser tenidos en cuenta a la hora de implementar una medida procesal de estas características.

Comencemos por las billeteras virtuales que son prestadas por distintas plataformas (vía web o a través de una aplicación móvil). Imaginemos que estamos frente a un caso en que la persona investigada tiene resguardadas sumas de bitcoins en una o más de ellas. Naturalmente, el camino a seguir sería contactar al proveedor de este servicio y ordenarle que bloqueara el acceso a su cuenta; y que disponga de los fondos que allí almacena acorde a lo que se entendiera más acertado (que inmovilice y conserve la suma de bitcoins; que la transfiera a alguna 'dirección bitcoin' administrada por el órgano a cargo de la investigación; que la cambie, a precio de mercado, por alguna moneda de curso legal y ponga a disposición el monto obtenido; o bien que intercambie sus unidades de valor por lo que se denomina una *stablecoin*, esto es, una 'moneda virtual' atada al valor del dólar estadounidense).

De lo contrario, será cuestión que esta persona —o alguien de su entorno que cuente con las credenciales de ingreso a su cuenta en la plataforma, que en muchos casos no es más que un nombre de usuario y una contraseña **(32)**— acceda a esta última y ponga a resguardo las sumas de bitcoins almacenadas por medio de una transferencia hacia otra cartera.

Más allá de las distintas variables que puede presentar este escenario, quizás la mayor dificultad se centra en conocer qué plataformas utiliza la persona investigada para resguardar fondos (no así su identificación en ella, ya que la mayoría de las plataformas serias, tanto a nivel local como internacional, en las que uno regularmente podría confiar para almacenar importantes sumas de bitcoins, aplican una política de 'Know Your Customer' - 'conozca a su cliente'). Indudablemente, será de utilidad el empleo de técnicas informáticas que permitan recuperar y analizar el historial de navegación que presentan los equipos que aquel pudo haber utilizado, o bien las aplicaciones móviles descargadas que se hallaban operativas. También será importante conocer de manera actualizada qué requisitos exigen las plataformas para operar a través de ellas y entablar, como ya se explicó, un canal de comunicación directo y ágil con las empresas que las administran, de forma tal de poder actuar rápidamente.

Ahora bien, un escenario totalmente distinto se presentará si la persona investigada utiliza como 'billetera' un programa instalado en algún dispositivo local (computadora de escritorio y/o portátil). Tal como se señaló en la nota al pie respectiva, habrá que tener presente que casi todas las carteras de este estilo ofrecen una metodología sencilla para, ante cualquier eventualidad, regenerar la billetera en otro equipo o migrar las direcciones hacia otra cartera (y, por ende, los fondos enlazados en ella). Algunas exigen, para ello, recordar únicamente doce palabras que conforman la denominada "semilla" o "clave maestra", ya que utilizan un esquema de derivación de carácter determinista. Otras, en cambio, generan en el propio equipo una copia de seguridad de las claves privadas, la cual fácilmente puede ser extraída y resguardada en algún dispositivo externo, como puede ser un pendrive, o en la 'nube' (*cloud storage*).

La cuestión es que llevar a cabo cualquiera de dichas acciones (regenerar la billetera en otro dispositivo o migrar las direcciones) no presenta mucha dificultad y dependerá, en definitiva, del grado de cuidado que cada usuario despliegue. Por tal motivo, si no se toman los recaudos necesarios, el secuestrar un equipo en el que pudiera haber operado alguna de estas billeteras, de por sí, no servirá de mucho, ya que fácilmente su dueño, aún sin acceso al

(32) Algunas plataformas ofrecen, además, la posibilidad de activar un doble factor de autenticación para acceder a la cuenta y/o concretar operaciones, generalmente asociado al teléfono celular del usuario (puede ser mediante el envío de un mensaje de texto o a través de un código que se obtiene por medio de una aplicación especial). En ese caso, el acceso de una persona ajena a la cuenta será sumamente difícil, ya que necesitará estar en poder del dispositivo asociado a ella.

mismo, podría disponer de los fondos almacenados en ella.

En el caso de las "billeteras frías", habrá que tener presente que muchos de los dispositivos físicos diseñados para almacenar claves privadas (tienen una figura similar a la de un pendrive) también pueden ser fácilmente regenerados en otro equipo **(33)**, por lo que tomar posesión de ellos, sin perjuicio de la dificultad que puede conllevar manipularlos, ya que casi todos cuentan con una mínima barrera de seguridad como puede ser un PIN o una clave privada, no asegura un control de los fondos.

Por su parte, en lo que respecta al papel impreso o manuscrito que cumple idéntica función (lleva anotada la dirección Bitcoin con su respectiva clave privada), quizás lo más aconsejable es, de lograr su incautación, disponer inmediatamente de los fondos enlazados en la respectiva dirección, concretando una transferencia hacia una cartera controlada por quienes llevan adelante la investigación; de lo contrario, cualquiera que cuente con una copia de aquel (ya sea la misma persona investigada o alguien de su confianza), podrá hacer exactamente lo mismo.

Intentaré sintetizar lo expuesto con el ejemplo de un caso real, que tuvo lugar recientemente en los Estados Unidos de América. Según informaron los distintos canales de noticias especializados en la materia **(34)**, en el marco de una investigación en la que intervinieron diversas agencias federales, fueron detenidas dos personas acusadas de haber participado de uno de los *hackeos* más importantes en la historia del ecosistema Bitcoin, el cual se llevó a cabo en el año 2016 en la plataforma (*exchange*) denominada Bitfinex e implicó el robo de fondos por un valor actual de 4.5 billones de dólares estadounidenses (119.754 unidades de bitcoins). Al parecer, habrían sido individualizadas luego de intentar 'blanquear' una pequeña parte de esos fondos a través de diversas transacciones financieras (movieron los bitcoins de una dirección a otra, con la finalidad de dificultar su rastro, hasta finalmente almacenarlos en una cuenta abierta a su nombre en un reconocido *exchange*, desde la cual realizaron pagos en tiendas comerciales y entidades financieras con el objeto de adquirir ciertos productos).

Lo relevante es que los investigadores habrían logrado incautar en uno de los procedimientos ejecutados la suma aproximada de 95.000 bitcoins, los cuales estaban inmovilizados en más de dos mil 'direcciones bitcoin' diferentes. ¿Cómo fue posible? Conforme se explica en la publicación, aparentemente, tras lograr acceder a los distintos archivos que una de estas personas resguardaba en la 'nube', advirtieron que en uno de ellos había un listado en el que se individualizaba cada una de estas direcciones, con su respectiva clave privada, por lo que inmediatamente, con autorización judicial, tomaron control de esas unidades de valor y las transfirieron hacia una 'cartera' propia.

En definitiva, cada escenario exhibe particularidades distintas que obligan a adoptar estrategias de actuación completamente diferentes, por lo que si se quiere tener éxito en la implementación de una medida cautelar que apunte a incautar sumas de bitcoins (en realidad, como se dijo, a tomar control de ellas sin que otro lo pueda hacer), la recomendación es que su planificación prevea de antemano todas las dificultades que se puedan presentar.

III. Reflexión final

Este trabajo nace con un riesgo ínsito, propio de toda producción académica que intente abordar temas vinculados al mundo de la tecnología. Concretamente, que al momento de su publicación pierda actualidad y, por consiguiente, que las ideas, conclusiones y herramientas que aquí se comparten carezcan de vigencia, o bien, simplemente, de utilidad, producto de alguna modificación sustancial que pudiera suscitarse en el plano de la realidad. Recordemos que el tiempo en esta área de conocimiento es efímero

(33) Los dispositivos más populares, conocidos bajo el nombre comercial de "Ledger" y "Trezor", en sus distintos modelos, utilizan como vía para 'regenerar' la cartera en otro equipo (ante la posibilidad de un eventual daño, pérdida, robo o cualquier otro incidente que de alguna manera exponga a un riesgo de filtración la información allí resguardada) una "semilla" conformada por 24 palabras claves, extraídas en forma aleatoria de un diccionario y cuya colocación debe respetar el orden asignado.

(34) https://www.bloomberg.com/opinion/articles/2022-02-09/business-rapper-was-bad-at-bitcoin-laundering.

y lo que hoy sirve o es práctico, mañana mismo puede dejar de serlo.

Sin ir más lejos, si uno estudia el último reporte publicado por la empresa Chainalisys Inc., dedicada, como se dijo, a ofrecer soluciones en análisis y búsqueda de datos en blockchain (como la herramienta de trackeo de transacciones que aquí se mostró) a instituciones financieras, agencias de gobierno y compañías que prestan servicios en materia de cripto-monedas, encontrará que allí se advierte de una mutación en el comportamiento de los criminales a la hora de 'mover' fondos originados en el marco de alguna actividad delictiva —ello, claro está, con la finalidad de romper su seguimiento e iniciar el proceso de conversión a dinero fiduciario—. Puntualmente se ha alertado sobre la adquisición cada vez más frecuente de tokens monetizados de protocolos De-Fi ('finanzas descentralizadas'), un ecosistema muy particular en el que se busca desarrollar servicios financieros sin intermediarios y en el que funcionan *exchange*s (denominados DEX) que operan, precisamente, con esa característica, esto es, sin ninguna persona o empresa detrás que los administre —utilizan 'contratos inteligentes' que ejecutan órdenes de transacciones en forma automatizada a partir de una programación de origen—, lo que permite que impere en ellos un total anonimato.

Es evidente que estas nuevas modalidades de flujo de 'valor digital' requieren, en lo que respecta a su abordaje desde el campo de la investigación penal, un estudio personalizado de cada una que permita desarrollar, frente a su empleo en la actividad criminal, herramientas propias de respuesta eficaz, las que pueden presentar, o no, coincidencias con las que aquí se proponen para el Bitcoin en particular.

Sin embargo, también es cierto que todas ellas (cripto-monedas, tokens monetizados) forman parte de una misma 'película' que ha venido a cambiar para siempre el sistema financiero, por lo que, más allá de que su 'salida a escena' tenga lugar en momentos distintos y bajo formatos diferentes, es muy probable que los conocimientos que se incorporen respecto de una sirvan para enriquecer y facilitar el abordaje de otra. De hecho, muchas comparten una misma raíz (la tecnología blockchain) y las diferencias que presentan entre sí, en algunos casos, no han sido más que pequeños cambios introducidos con el objeto de mejorar algún rasgo específico de un protocolo ya existente.

Por ese motivo, confío en que este trabajo, de alguna u otra manera, podrá ser de utilidad para al lector, ya sea como guía de ayuda u orientación en el tratamiento de un caso concreto, o bien como incentivo para la búsqueda de nuevos y mejores canales de abordaje; máxime tratándose de una temática tan dinámica como actual.