Técnicas de Investigación de Fraudes con Criptomonedas

Podesta Ariel[1], Lamperti Sabrina[2], Giaccaglia Fernanda[3], Giovaneli Maria Eugenia[4], Almirón Sebastián[5]

[1] Universidad FASTA, apodesta@ufasta.edu.ar
[2] Universidad FASTA, slamperti@ufasta.edu.ar
[3] Universidad FASTA, fernandag@ufasta.edu.ar
[4] Universidad FASTA, eugeniagiovaneli@ufasta.edu.ar
[5] Universidad FASTA, salmiron84@gmail.com

Abstract. Este trabajo trata las dificultades que deben enfrentar los investigadores en casos de fraude con criptomonedas. La naturaleza de este ecosistema de activos es diferente a la del dinero FIAT[1] convencional. A nivel técnico funciona de una manera radicalmente distinta, y a nivel jurídico siempre hay vacíos legales. Eso sumado a su repentina aparición y a la velocidad de su evolución, deja al investigador falto de suficientes herramientas para llegar al éxito en su labor.

En ese escenario, el investigador debe lidiar con una serie de complicaciones que lo obligan a instruirse permanentemente o quedarse afuera del dominio en la temática. Ejemplo de dichas complicaciones pueden ser: tecnologías que día a día agregan nuevos servicios no regulados, entidades de intercambio de criptomonedas que aparecen y desaparecen sin estar vinculadas a un lugar físico, mecanismos de suscripción y operatoria no estandarizados ni legalizados, cuentas absolutamente anónimas, jurisdicción insuficiente, entre otras.

De ese modo el propósito de este trabajo es reducir esa brecha de desconocimiento que deja en desventaja a los investigadores frente a este tipo de fraudes.

Keywords: Investigación, Fraude, Criptomonedas.

1. Introducción

Las criptomonedas han aparecido hace unos diez años, y si bien su uso aún permanece acotado a un sector de la sociedad que está involucrado en la temática, cierto es también que su popularización no tardará en llegar, impulsado por la dinámica que es propia de las inversiones y que buscan hacer las personas en pos de una mejora de su situación económico-financiera.

[1] También conocido como dinero por decreto, es una forma de dinero sin valor intrínseco. Su valor se basa en su declaración como dinero por el Estado. Es dinero de curso legal cuyo valor no deriva del hecho de ser un bien físico o mercancía, sino por ser emitido y respaldado por un gobierno.

Claramente es una temática que, por su repentina aparición, muchos desconocen total o parcialmente y va de la mano con la falta de regulación normativa, que requiere tiempo para ser establecida y que no puede reaccionar a cambios tecnológicos con tanta celeridad. Ello sin perjuicio de la sanción o dictado de algunas leyes que, de manera reactiva, comienzan a aparecer en pos de cubrir vacíos que pueden acarrear su aprovechamiento por parte de sujetos que buscan de alguna forma, evadir impositivamente al Estado.
Por ejemplo, la ley 27430 incorpora el tratamiento de las monedas digitales en el impuesto a las ganancias, pero éste presenta inconsistencias legales difíciles de resolver sin merma de los principios de legalidad y de razonabilidad, producto de una legislación prematura que trata con avidez recaudatoria un fenómeno aún incipiente, de un potencial económico y social aún desconocido para el legislador y hasta para sus propios desarrolladores. Si bien se las pretendió asimilar a las ganancias derivadas de inversiones en títulos valores con cotización, el resultado obtenido es absolutamente dispar, complejo de interpretar e impreciso.
Es notoria la falta de una definición o caracterización legal sobre qué debe entenderse por "monedas digitales" en la narración de la reformada ley de impuesto a las ganancias, y con mayor razón, ocurre con las "criptomonedas".
En un marco de tanta ausencia de claridad, es lógico que el delincuente digital encuentre sistemáticamente oportunidades de realizar fraudes eludiendo la justicia, y cumplimentar su cometido sin recibir pena alguna. Así, el propósito de este trabajo es aportar conocimiento en la temática, que le permita al investigador contar con un mayor número de herramientas a la hora de realizar su labor.
Aclaración: Todos los conceptos técnicos aquí tratados, respecto de criptomonedas y Blockchain, toman como esquema de referencia a Bitcoin y su propia blockchain. Esto es debido a que es la primera de esta nueva generación de activos digitales descentralizados, y que el resto de las conocidas socialmente como "criptomonedas" han sido basadas mayormente en sus planteos conceptuales. Por otra parte sería imposible enumerar los aspectos que las distinguen entre sí, siendo que a la fecha existen más de 7000 (siete mil) criptomonedas en el mundo.

1.1. Características de las criptomonedas

Para hablar de criptomonedas debemos previamente conocer las características del dinero y del dinero electrónico.

Para SAMUELSON y NORDHAUS[2] el dinero es «todo lo que sirva como medio de intercambio de aceptación común». El dinero no se busca por sí mismo, sino por las cosas que pueden comprarse con él. Es por ello que sostienen que el dinero es todo lo que se acepta normalmente como medio de cambio y que a diferencia de otros bienes económicos, el dinero vale por convención social
El dinero, representado en monedas y billetes, no tiene valor en sí mismo, pues su valor radica en las cosas que se puedan comprar con él; es decir, su valor radica en lo que se puede hacer con él.

[2] SAMUELSON, P. y NORDHAUS, W. (2006). Economía. (18o ed.). México: McGraw Hill. pp. 30 y 491.

Propiedades del dinero. La función elemental del dinero es la de intermediación en el proceso de cambio. El hecho de que los bienes tengan un precio proviene de los valores relativos de unos bienes con respecto a otros.
La causa de estas relaciones se origina en la comparación del valor de los bienes y en las contingencias del mercado. La fuente de esos valores puede ser el trabajo incorporado en esos bienes o la utilidad que le atribuyen los individuos, según nos orientemos a una teoría objetiva o subjetiva del valor.
Como ya se mencionó anteriormente, el dinero permite el intercambio de bienes y servicios en una economía de una manera más sencilla que el trueque.
Por tanto, para que un bien pueda ser calificado como dinero se deben satisfacer las siguientes tres propiedades y que son las tres principales funciones que cumple el dinero en un sistema económico moderno:

- **Medio de intercambio:** para evitar las ineficiencias de un sistema de trueque. Cuando un bien es requerido con el solo propósito de usarlo para ser intercambiado por otras cosas, posee esta propiedad. Por ejemplo, pocas personas conservan billetes para colección. En cambio, la mayoría de las personas los conservan por la posibilidad de intercambiarlos cuando lo deseen por otros bienes. Además, el dinero debe ser un bien ligero y fácil de almacenar y de transportar.
- **Unidad contable:** Cuando el valor de un bien es utilizado con frecuencia para medir y comparar el valor de otros bienes o cuando su valor es utilizado para denominar deudas, se dice que el bien posee esta propiedad. Por ejemplo, si los miembros de una cultura se inclinan por medir el valor de las cosas en referencia a las vacas, las vacas serían la principal unidad contable. Un caballo podría costar 10 vacas y una cabaña unas 45 vacas. La unidad de cuenta significa que es la unidad de medida que se utiliza en una economía para fijar los precios.
- **Medio de almacenamiento de valor:** Cuando un bien es adquirido con el objetivo de conservar el valor comercial para futuro intercambio, entonces se dice que es utilizado como un depósito de valor. En el ejemplo anterior, una vaca tendría un problema a la hora de servir como dinero, puesto que es un bien perecedero: con el tiempo muere. Otros materiales, como el oro y la plata, conservan sus propiedades a pesar del paso del tiempo. Es un medio de acumulación o atesoramiento. El dinero, como representante de la riqueza, tiene el poder de comprar cualquier mercancía y se puede guardar en cualquier cantidad. En otras palabras, la función de atesoramiento sólo puede realizarla el dinero de pleno valor: monedas y lingotes de oro, piedras preciosas, objetos de oro, etc. El bien escogido como medio de acumulación o almacenamiento debe ser siempre algo que pueda guardarse durante largos periodos sin que se deteriore. El dinero es un depósito de valor pero no el único, cualquier activo que mantenga su poder adquisitivo a lo largo del tiempo servirá como depósito de valor.

Además de los puntos anteriores, el dinero debe ser reconocido por la sociedad que lo usa, permitiendo su identificación y valoración de una forma clara. El dinero, tal como lo conocemos hoy (billetes y monedas sin valor propio), debe estar avalado o certificado por la entidad emisora. Actualmente son los gobiernos, a través de las leyes,

quienes determinan cuál es el tipo de dinero de curso legal, pero son otras entidades, como el Banco Central (BCRA) y la casa de la moneda , los que se encargan, primero, de regular y controlar la política monetaria de una economía, y segundo, de crear las monedas y billetes según la demanda y la necesidad de tener dinero físico.

El dinero electrónico tiene su justificación en el auge que ha tenido la electrónica en la vida actual; consiste en que las personas podrán hacer sus pagos sin necesidad de tener especies monetarias. Es una representación electrónica del dinero. Por lo tanto, para que un medio de pago pueda considerarse dinero electrónico debe almacenar efectivamente un valor que cumpla con todas las propiedades del dinero.

Propiedades del dinero electrónico. Las transacciones, en general, y las de dinero electrónico en particular deben cumplir con las siguientes propiedades denominadas ACID (sigla que significa *Atomicity, Consistency, Isolation, Durability* o, en español, Atomicidad, Consistencia, Aislamiento y Durabilidad), que se suman a las propiedades del dinero antes explicadas:

- **Atomicidad:** cualquier cambio de estado que produce una transacción es atómico. Es decir, ocurren todos o no ocurre ninguno. En otras palabras, esta propiedad asegura que una operación se realiza o no se realiza, por lo tanto no puede quedar el sistema a medias. Por ej: si transfiero fondos de una cuenta a la otra, implica que se debitará el importe a transferir de la primer cuenta y se acreditará en la segunda. Si se produce un corte en el medio de la transacción, se vuelve atrás, es decir, o se realiza completa la transferencia o no se realiza.
- **Consistencia:** propiedad que asegura que una transacción no romperá con la integridad de una base de datos, pues respeta todas las reglas y directrices de ésta.
- **Aislamiento:** propiedad que asegura que no se afectarán entre sí las transacciones. En otras palabras, dos o más transacciones sobre los mismos datos no generarán un problema.
- **Durabilidad:** propiedad que asegura la persistencia de una transacción, es decir, una vez que la transacción quedó aceptada no podrá deshacerse aunque falle el sistema.

En informática, estas propiedades “ACID” son un conjunto de características que garantizan que las transacciones en una base de datos son fiables. En el contexto de bases de datos, una transacción es una única operación sobre los datos.

Un ejemplo de una transacción más compleja es la transferencia de fondos de una cuenta a otra, la cual implica múltiples operaciones individuales. Si un sistema supera la prueba ACID, significa que es fiable.

Las criptomonedas, en cambio, son activos virtuales cuyo valor está dado por la oferta y la demanda. Rápidamente vemos que no cumplen con algunas de las características antes enunciadas. No tienen una entidad específica que regule su expedición y control, por lo que **no cumple con la propiedad de ser socialmente aceptado**. Veamos también con relación a las restantes características.

Como se indicó precedentemente el dinero, desde el punto de vista económico, tiene básicamente tres funciones: medio de pago, unidad de medida y medio de acumulación del valor. A continuación vamos a analizar el cumplimiento de cada propiedad:

Medio de pago. Lo más sencillo de afirmar es que las criptomonedas funcionan como medio de cambio, ya que pueden ser aceptadas como medio de pago a cambio de bienes o servicios. Sin embargo, dicho uso está lejos de ser adoptado por las masas y la aceptación en los intercambios no está presumida. Solo podrán ser utilizadas como medio de cambio cuando haya un acuerdo entre las partes de que ese método será aceptado.
Asimismo, debido a su carácter volátil, las criptomonedas son percibidas más como una oportunidad de inversión especulativa que como medio de pago.

Según Andrei Boar[3] hay tres inconvenientes en el uso de criptomonedas como medio de pago: la demora en la validación (comprobación de la transacción) que puede durar hasta diez minutos; el miedo a un activo que se desconoce y el poco uso en el comercio.

Unidad de medida. Se visualiza la alta volatilidad de las criptomonedas como una debilidad para que se tomen como unidad de medida. Considerando que la volatilidad es una medida de la frecuencia e intensidad de los cambios del precio de un activo en un horizonte temporal específico, podemos afirmar que las criptomonedas se enfrentan a grandes cambios en su valor como consecuencia del juego entre oferta y demanda. Es por ello, que al día de hoy, es difícil pensar que se utilice como unidad de cuenta, ya que los precios se expresan en otra moneda, como el dólar o una moneda local, y ese precio se convierte a una determinada cotización de bitcoin.

Medio de acumulación de valor . Si bien las criptomonedas son utilizadas en gran medida como inversión ya que el valor tiende a subir, esto no significa que sea un depósito de valor útil. El concepto de depósito de valor está mayormente relacionado a la posibilidad de poder mantener un valor en el tiempo para ser utilizado en un tiempo futuro. En el caso de las criptomonedas, no hay una función de asegurar un valor y poder utilizarlo en un momento futuro, ya que sus cambios drásticos impiden esa función de seguridad.

El funcionamiento de las criptomonedas se sostiene gracias a dos elementos esenciales: la *blockchain* – o cadena de bloques- y la actividad de los mineros. Las criptomonedas, por tanto, tienen características propias que las diferencian de una moneda en sí, y que permiten definir su naturaleza jurídica.

[3] Boar, Andrei: “Descubriendo el Bitcoin” - Ed. Profit - 2018

2. Conceptos esenciales sobre criptomonedas

2.1. Principios Originarios

Es importante tener siempre presente los principios esenciales con los que fueron creadas las criptomonedas. Ellos son los que definen su funcionamiento, independientemente de la plataforma tecnológica con la que se opere. Determinan los límites y alcances que el investigador puede tener en un caso de este ámbito. Podrán representar tanto dificultades como ventajas, pero el provecho que se le saque dependerá del conocimiento que tenga la persona sobre los mismos.
Se observan a continuación:

Descentralización. Posiblemente el principio más representativo del mundo de las criptomonedas. Su significado concreto es evitar que exista una entidad que centralice el dominio sobre los activos. Aquí no hay ni una empresa ni un banco que pueda gestionar el sistema, ni que pueda regir arbitrariamente sobre el mismo. El congelamiento de las cuentas, o las restricciones en transferencias, son algo que simplemente no tiene lugar. No hay quien castigará o recompensará en caso de buena o mala conducta. La libertad de movimiento y atesoramiento es inalienable.
Visto desde ese punto de vista parece ser un gran beneficio para el usuario común. Pero la contrapartida a todo esto es que tampoco existe un "a quien reclamar". Esto agrega un riesgo que la persona no siempre está dispuesta a aceptar. El hecho de no tener un "interviniente" en caso de conflicto es verdaderamente un problema. En efecto, el ahorrista no tiene respaldo alguno ante cualquier imprevisto.
Esta ausencia de "entidad interviniente" se hace aún más problemática en el ámbito de la justicia. Ante un delito económico, una de las primeras acciones a tomar es evitar que el dinero involucrado sea gastado o transferido. Esto, en el sistema monetario convencional normalmente se realiza a través de los bancos, congelando las cuentas. Pero en el mundo de las criptomonedas puede no ser posible, si la cuenta no pertenece a ninguna entidad administradora, como lo son los "exchanges"[4].
Con este planteo, la descentralización es claramente una desventaja para la Justicia. Pero no hay que limitarse a pensarlo solo de ese modo. La "descentralización" también trae un concepto implícito que es la "distribución". Y en este caso, la distribución es de la información de las transacciones mismas. Esto implica que si bien no hay una entidad centralizada a quien acudir para solicitar información, sí hay una forma de obtenerla. La forma es integrarse a la red y recibir los datos que por naturaleza son compartidos. Es tan simple como tener al alcance de la mano la información de todas las transacciones que alguna vez sucedieron históricamente.
Así es como este principio de "descentralización" se presenta como desventaja o ventaja según el enfoque y provecho que se le sepa dar.

[4] Entidad que permite operar con criptomonedas, entre otros activos. Suelen ser accesibles a través de su propio sitio Web y para obtener una cuenta de usuario habitualmente requieren una validación de identidad.

Anonimato. Éste es tal vez otro de los aspectos más relevantes buscados en este sistema, pero no es exactamente el "anonimato" sino la "privacidad". Ese fue el verdadero objetivo. Y esta privacidad es en términos de la "identidad" de la persona, de forma tal que solo ella pueda decidir si revelarla o no.
Dado que en el esquema de criptomonedas todas las transacciones son puramente visibles, era evidente que debía existir una forma de encapsular los datos de origen y destino de cada una de ellas. Así es como surge el concepto de *wallet* (o "billetera", en español), que a los fines prácticos es un concepto análogo al número de cuenta bancaria. La diferencia es que aquí no hay una forma natural de asociar una *wallet* a su verdadero dueño. El sistema mismo no fue diseñado así. Para ello encontraremos ciertos métodos, que son mencionados en la sección "Guía de recomendaciones". De todas maneras, son efectivos solamente porque en el esquema de suscripción se agregan intermediarios, que no son realmente necesarios. Éstos, son entidades que facilitan los mecanismos de acceso al mundo de criptomonedas, a cambio de que el individuo brinde su verdadera identidad, entre otras cosas. Pero no por ello significa que el sistema haya sido diseñado originalmente así. Habrá entonces ciertos usuarios que no sea posible identificar su verdadera identidad.
El problema con esto es que en el ámbito de la Justicia, el anonimato siempre es un enemigo. El ciber-delincuente busca imperiosamente ser furtivo, no ser identificado. Y en un esquema que fue ideado desde su principio para dar lugar a ello, su actividad fraudulenta se ve beneficiada.
En todo este contexto, es evidente que el principio de "privacidad" o "anonimato" es más un perjuicio que un beneficio para el investigador judicial.

Seguridad. Este aspecto se buscó en base a dos objetivos. Por un lado lograr que el propietario de una cuenta (*wallet* en este caso) tenga la garantía de que solo él pueda operar con ella. Y por otro en que el registro de transacciones no pueda ser alterado en el tiempo. Ambos fueron logrados principalmente a través del uso de algoritmos criptográficos.
El primero de ellos se cumple mayormente gracias a los mecanismos de "clave privada" y "clave pública". A grandes rasgos, la clave privada sirve para operar con la cuenta y la pública para verificar la legitimidad de sus transacciones. El punto aquí es que quien posea la privada tendrá pleno dominio sobre la cuenta y mientras no la comparta seguirá siendo así. Esto, a los fines de la Justicia, es nuevamente un desafío puesto que no es posible bloquear ninguna transferencia. Basta con que el dueño registre una transacción a cualquier destino, haciendo uso de su clave privada, para que los activos sean transferidos.
El segundo de ellos, que refiere a la inalterabilidad de los datos, se logra a través de la concatenación de registros, donde la integridad de uno depende siempre de sus predecesores. De esta forma, alterar uno de ellos no es posible sin hacerlo con los subsiguientes para mantener la consistencia en la cadena. Y para ello debe cumplirse con una serie de requisitos criptográficos que demandan una potencia de procesamiento que ningún equipo conocido posee actualmente. Por otra parte, no basta con lograr alterar los datos en un equipo sino que debería hacerse lo mismo en la mayoría de ellos. Hay que recordar que la esencia de este tipo de sistemas es la distribución, y que se operará según lo que la mayoría diga.

Sabiendo esto, los investigadores judiciales no deben enfocarse en prevenir los envíos, ya que no pueden, sino en recordar que todo queda registrado y la fidelidad de la información es casi incuestionable. Ergo, no importa cuantas veces se redirijan los fondos, siempre habrá un modo de ver una trazabilidad en la concatenación de las transacciones. Esto podría ayudar significativamente en el rastreo de la actividad.

Deslocalización. El enfoque de este principio es que el alcance de las transacciones trascienda los límites geográficos. Básicamente, que no existan limitantes para transferir activos a cualquier punto del planeta.
Esto se da en forma natural a partir del paradigma de esta tecnología. Cada participante desconoce dónde se encuentra el resto. Él solo sabe que se comunica con otros nodos a través de Internet. Y ni siquiera lo hace con todos. Solo se interconecta con algunos y a través de ellos tiene un conocimiento indirecto de lo que el resto está procesando.
Bajo esa configuración cada participante lleva una copia del histórico completo de transacciones. Pero desconoce a ciencia cierta tanto la ubicación geográfica del resto de los nodos como de los usuarios reales del sistema (personas físicas). Él solo actualiza su registro en función de las nuevas transacciones que le van llegando.
Teniendo en cuenta entonces que se trata de un sistema donde por naturaleza la localización física no se registra, entonces es natural que no existan limitantes para el acceso al mismo desde cualquier punto del planeta. Con lo cual, no es necesario ni siquiera transferir activos para que ellos estén disponibles en otro país, por ejemplo.
Esto agrega complejidad a las investigaciones judiciales ya que, en este esquema, el ciber-delincuente siempre tiene acceso a sus activos sin importar donde se encuentre.

2.2. Conceptos básicos de utilidad

A continuación se listan algunos conceptos básicos de utilidad en esta temática:

- ***Exchange**:* Entidad que permite operar con criptomonedas, entre otros activos. Suelen ser accesibles a través de su propio sitio Web y para obtener una cuenta de usuario habitualmente requieren una validación de identidad. Una vez obtenida es posible comprar, vender, recibir, enviar criptomonedas, o incluso intercambiarlas por otras.
  Este tipo de entidades tienen un rol sumamente protagonista en el ámbito de las investigaciones judiciales de fraudes con criptomonedas.
  Ejemplo de uno de ellos: https://www.binance.com/
- ***Wallet**:* También llamada “billetera virtual”, es a grandes rasgos, es el análogo de “cuenta bancaria”. El identificador de una *wallet*, es lo que se utiliza para realizar un envío, como destino de los activos. Ejemplo:
  1GVY5eZvtc5bA6EFEGnpqJeHUC5YaV5dsb
  Como puede observarse, se compone de una secuencia de caracteres que combina números y letras.
- ***Hot Wallet:*** Es una *wallet* que se encuentra alojada en un sistema permanentemente conectado a Internet. Este tipo de *wallets*, son comúnmente provistas por los *exchanges*, quienes disponen del equipamiento suficiente

para mantener en línea un sistema de intercambio de cripto divisas las 24 hs del día.

- ***Cold Wallet:*** En contraposición con las anteriores, son *wallets* que solamente se conectan para transaccionar y luego se desconectan. Habitualmente son administradas por software instalado en computadoras personales o dispositivos móviles.
- **Clave Privada:** Podría considerarse como un concepto análogo a la "clave de acceso" a una cuenta bancaria. Pero es aún más que eso. La clave privada permite el control absoluto sobre una *wallet*, sin restricciones. No hay forma de prevenir una transacción si se dispone de ella.
  Esencialmente es una secuencia de caracteres, que sirven para "firmar digitalmente" transacciones desde una determinada cuenta.
  Ejemplo: 16qT2iLQ7d5MiEkKWYau6mfRNHUFZ3NzHz
  Cuando la firma es validada la transacción se considera realizada, sin ningún otro requisito.
  Por otra parte, la clave privada sirve para generar la "clave pública" (definida a continuación), y la *wallet* que se corresponde con dicha clave privada.
- **Clave Pública:** Es un valor que permite validar la firma digital de las transacciones que corresponden a determinada wallet. En esencia es también una secuencia de caracteres, similar a la clave privada.
  Ejemplo:
  0377a8565da9e67632a6b27a31548b043b510efdd5b5108dc2203fac57cb239fd0
  A través de un algoritmo de verificación de firma, se utiliza esta clave pública para determinar la autenticidad de todas las transacciones que salen de una *wallet.*
- ***Hash***: Es el valor resultante de un cálculo algorítmico que se realiza sobre un contenido digital. Dicho valor tiene una longitud fija, y es unívocamente representativo del contenido digital, de tal forma que un cambio menor en este último produciría un cambio significativo en el valor de *hash*. Esto permite detectar adulteraciones inmediatamente.
  En el ámbito de las criptomonedas, esto se utiliza mucho para impedir que se produzcan modificaciones en los registros de transacciones, sin ser detectadas.
- **Transacción**: En el contexto de las criptomonedas, una "transacción", no es más que el envío de cierto monto de activos a una o más *wallets.*
- **Bloque**: Las transacciones son registradas en el registro global a medida que ocurren. Pero no lo hacen de a una, sino por "bloques", que no es ni más ni menos que una cierta cantidad de ellas que se registran todas juntas en un mismo paso. Dicha cantidad es variable y depende de la demanda de los usuarios.

2.3 Funcionamiento General

Antes de analizar casos puntuales es fundamental entender cuál es la idea base de esta tecnología. Luego será mucho más sencillo entender cuestiones específicas.

Concepto de "registro". El primer concepto a tratar es que las criptomonedas se erigen en base a un "registro". Su base de datos es un registro. Es comparable a una hoja (o muchas de ellas), en la que en cada renglón se anota una nueva información. Pero nunca se eliminan los anteriores, funciona por agregación.
Esto empieza a evidenciar uno de sus aspectos más conocidos, que es su "inalterabilidad". Una vez registrada la información ya nunca se elimina ni se modifica.
Otro aspecto que se desprende de lo anterior es que es una base creciente. Su información nunca deja de acumularse. Ergo su tamaño en un determinado momento siempre será mayor al del instante anterior.
Por otra parte, si nunca se eliminan datos, entonces quiere decir que el histórico completo siempre estará allí disponible, y en efecto, por ejemplo en Bitcoin esto ocurre así. Siempre tenemos acceso a cualquier operación efectuada en cualquier punto del tiempo, incluida la primera de todas.

Concepto de "registro de transacciones". La siguiente noción a agregar es que es un "registro de transacciones". Todo lo que se almacena en él son únicamente transacciones. Y ellas representarán movimientos de criptomonedas entre distintas cuentas. Podrían imaginarse como por ejemplo: "transferir x Bitcoins de la cuenta A a la B". Si eso es lo que almacena el sistema, entonces también hay otros conceptos que se pueden inferir.
En primer lugar, no existe el registro de la "cuenta". Solo hay movimientos entre cuentas, pero no cuentas. El saldo de cada una de ellas solo se deduce según las operaciones que las involucran. Pero no está el valor específico en un registro puntual.
Esto hace que su seguridad se incremente, puesto que alterar un saldo es mucho más difícil que modificar un valor. En primer lugar, como se vio previamente, alterar un valor ya registrado no es posible, no es una función válida en Bitcoin. Y en segundo lugar, todo cambio en un saldo se debe corresponder con una transacción legítima, y esto conlleva robustos procesos de verificación.
Otro aspecto a analizar es que si solo hay transacciones, entonces inevitablemente ellas deben referenciarse entre sí para saber de dónde proviene el dinero (las criptomonedas). No pueden referir a saldos en cuentas dado que ese dato no existe, como se mencionó previamente. Ahora, si también supiéramos que contamos con el registro histórico de operaciones completo, entonces siempre será posible hacer un análisis de concatenación de movimientos hasta la misma primera transacción que ocurrió en todo el sistema. Esto puede ser realmente útil en ámbitos judiciales donde se investiguen los orígenes de determinados fondos.
Otro concepto que se deduce es que "solo hay criptomonedas". El propósito de las transacciones es enviar criptoactivos de una cuenta a otra y solamente ese. Ningún otro activo está involucrado en esta red. De modo que cuando se habla de dólares en determinada cuenta de Bitcoin, se está haciendo implícitamente una traducción de Bitcoins a dólares, según su cotización actual.
Finalmente, la idea a denotar es que "todo tiene su origen". No es posible tener un monto que no refiera a una transacción. Su programación misma no lo permite. De ese modo, siempre se tendrá un claro conocimiento de las criptomonedas en existencia en todo el sistema.

Concepto de "registro de registro de transacciones distribuido". La característica de "distribuido" es lo que mayormente amplifica el nivel de seguridad que ofrece el esquema. En las criptomonedas, "distribuido" significa que cada participante tendrá una copia exacta del mismo registro que el resto tiene.
Cada una de las transacciones que se genera es replicada en tiempo real en todas las copias del registro alrededor de todo el mundo. De ese modo existen tantos puntos de validación como participantes en la red.
Esto significa que la adulteración de los datos en las criptomonedas se vuelve extremadamente difícil. Quien quiera cargar información falsa deberá atacar exitosamente a todas las copias de la red, y eso involucra un ataque masivo a nivel mundial. Es evidente entonces, que lograr este tipo de fraudes es una tarea que no está al alcance de una simple organización y que su probabilidad de ocurrencia se reduce a valores casi insignificantes.
A parte de esta cuestión de seguridad, existen otras ventajas que surgen de esta característica de ser "distribuido". Se enumeran a continuación:

Todos pueden tener una copia. Tener una copia del registro no tiene impedimentos. Cualquiera puede descargarlo y tenerlo localmente para lo que crea conveniente. De hecho, entre más participantes se agreguen a la red, más robustez gana el sistema.

Todos pueden validar transacciones. Si todos pueden tener una copia del registro entonces todos pueden determinar la legitimidad o no de las nuevas transacciones. Lo único que tienen que hacer es revisar los datos a los que hacen referencia y verificar si corresponde o no permitir estas nuevas transacciones. Ejemplo: negar un envío cuando no hay saldo disponible.

Todos pueden analizar la historia. El registro está completo, hasta la misma primera transacción que históricamente se efectuó. De ese modo, cualquier estudio que desee realizarse acerca de cualquier momento y cualquier cuenta, es posible realizarlo. La información está siempre disponible.

Todos pueden constatar la validez de su información. Si el registro es replicado entonces significa que todos deberían tener la misma copia. Ante la duda sobre determinada información, siempre será posible constatarla con la de otro participante. Si este discrepa entonces se revisa con los registros de un tercero. Sino con un cuarto, y así sucesivamente. Pero debido a que un ataque masivo es virtualmente imposible, siempre se llegaría a un consenso por mayoría en el acuerdo de determinada información.

3. Aspectos discutibles de las criptomonedas y fraudes típicos.

El incremento en la utilización del dinero digital y la tendencia a reducir el uso del dinero efectivo ha ocasionado un incremento en el empleo de criptomonedas como medios de pago en las sociedades. Es por ello que se han convertido en un tema de

interés para cada gobierno dado que constantemente buscan revisar las legislaciones sobre las operaciones con este tipo de tecnología.

El vacío legal que se ha producido entre el nacimiento de las criptomonedas y las diferentes posturas que cada gobierno ha adoptado frente a ellas, ha despertado un interés significativo en los piratas informáticos. Las amenazas de ciberseguridad han evolucionado rápidamente de la mano de las innovaciones tecnológicas aprovechando los vacíos legales.

Las criptomonedas hoy en día se relacionan con altas tasas de ganancias y existe un creciente interés de las sociedades en ellas. A medida que hay más gente interesada en las criptomonedas, los estafadores van encontrando más formas de usarlas y han aprovechado su desarrollo para desenvolver sus actividades ilegales.

La red *blockchain* en la que se basan no ha sido vulnerada, pero sí se han producido multitud de robos y de estafas en las plataformas que ofrecen servicios en este segmento del mercado.

Las estafas con criptomonedas suelen presentarse de distintas formas y en todas ellas la finalidad común es que el estafador quiere que se le envíe dinero, o se le haga un pago, con Bitcoin u otro tipo de criptomoneda, o bien apropiarse indebidamente de ellas.

Los principales fraudes se pueden resumir en los siguientes puntos:

- **Sitio web fraudulento:** Existe una gran cantidad de sitios web creados para ser una copia fiel de empresas originales y válidas. Incluso si el sitio tiene un aspecto idéntico al que cree que está visitando, es posible que lo dirija a otra plataforma para efectuar el pago. Por ejemplo, hace clic en un vínculo que parece un sitio legítimo, pero los atacantes crearon una URL falsa con un cero en lugar de la letra “o”.
- **Aplicaciones falsas:** Otro método común que utilizan los estafadores para engañar a los inversionistas de criptomonedas es a través de aplicaciones fraudulentas que se pueden descargar a través de Google Play y la App Store de Apple. Por ejemplo, puede ocurrir con aplicaciones que gestionen billeteras virtuales gestionadas por los ciberdelincuentes quienes a través de un *malware* se apodera de las criptomonedas.
- ***Ransomware:*** Utilizando un *software* malicioso que se instala en la computadora, los ciberdelincuentes secuestran datos de las organizaciones; los cuales mantienen cautivos hasta que se le pague un rescate, que por lo general, es en Bitcoin o alguna otra criptomoneda.
- **Códigos Maliciosos:** Haciendo uso de códigos maliciosos, el delincuente secuestra equipos ajenos para utilizar la computadora para realizar minado de monedas virtuales. Este proceso se lleva a cabo de forma oculta, pues pasa inadvertido para los usuarios del equipo.
- **Apropiación de las criptomonedas:** a través del acceso ilegítimo a la billetera y a la realización de operaciones desconocidas por el usuario titular.

4. Guía de recomendaciones

4.1. Revisión de Blockchain

Como se mencionó previamente, en los esquemas de criptomonedas, el registro de transacciones es globalmente compartido, público y de fácil acceso. El investigador puede y debe hacer uso de ello. En Bitcoin, por ejemplo, existen numerosos sitios gratuitos para este fin. Uno de ellos es https://www.blockchain.com/
Allí pueden realizarse diversas verificaciones, como ser:

- Saldo de una *wallet* (billetera virtual)
- Destino de envíos
- Dia y hora de transferencia
- Origen de los fondos enviados
- Secuencia de transacciones realizadas a partir de una de ellas
- Etc

En definitiva, todo el histórico transaccional está disponible. Cualquier búsqueda que desee realizar el investigador, podrá efectuarla.
Esto es la base de toda investigación sobre criptomonedas.

4.2. Identificación de entidades involucradas

A diferencia del sistema tradicional, en una transacción de criptomonedas, el origen y destino pueden ser entidades absolutamente desconocidas. No siempre existe ese banco o entidad financiera a la cual recurrir para solicitar información. Pero si existiera, es de vital importancia contemplarla para posibles consultas al respecto. Para ello, debe indagarse profundamente en todo lo que pueda aportar el damnificado, respecto de los movimientos que realizó.

El **origen** de una transacción puede corresponder a **una cuenta en un *exchange***, una **aplicación de PC** o **una de teléfono celular**.

El **caso del *exchange*** es indudablemente el más conveniente en las investigaciones, puesto que como se mencionó previamente, suelen solicitar una validación de identidad como requisito necesario para abrir una cuenta con ellos. Siendo así, la vía más directa para obtener información es a través de la justicia, enviando un pedido formal (“oficio”), que exija a la entidad la entrega de los datos solicitados.
Por ejemplo, podría consultarse el sitio https://www.walletexplorer.com/ que podría orientar sobre el origen de la *wallet* o su vínculo con un *exchange*.

¿Qué se puede solicitar?

- Confirmación de asociación de una billetera virtual a un usuario del *exchange*
- Identidad registrada para un usuario determinado
- Histórico de transacciones vinculado a una billetera virtual

- Histórico de operaciones para un usuario
- Cantidad de cuentas y billeteras asociadas a un usuario
- Y cualquier otra información que pueda tener registrada el *exchange.*

Como puede verse, es de extrema utilidad contar con la información que un *exchange* podría brindar. El escenario más complejo en este caso se da cuando la entidad no tiene su base central en el territorio nacional. Binance, por ejemplo. Allí, el éxito del pedido, dependerá tanto de los convenios de reciprocidad establecidos como de la buena voluntad de la entidad.

Cuando el **origen** de las transacciones es una **aplicación de PC o dispositivo móvil**, el escenario se vuelve más complejo. Debido a que en este caso quien tiene dominio sobre la *wallet* no es una entidad "visible" es mucho más difícil dar con el responsable.
Si el problema se produce en el equipo de la víctima, podría realizarse un estudio forense en búsqueda de evidencia digital que identifique un posible responsable. Suele ocurrir que ya sea por virus informático o bien por acceso indebido, se transfieren fondos de una *wallet* alojada localmente a un destino desconocido. El estudio forense podría esclarecer algo de lo sucedido.

Cuando el delito no involucra los dispositivos de la víctima, es cuando es realmente complejo hallar el responsable del fraude. Este tipo de casos suele darse cuando por alguna razón se accede ilegítimamente a una *hot wallet* y desde allí se transfieren los fondos. Por ejemplo, al obtener el acceso a la casilla de correo de la víctima es posible solicitar un "blanqueo" de contraseña en cualquier cuenta de criptomonedas asociada. Con el acceso a la cuenta se transfieren los fondos.
El mayor problema en este caso es que el destino suele ser una "cold wallet", que no se encuentra registrada en ningún *exchange*. Y esto impide la obtención de cualquier dato, como la identidad del responsable o hasta incluso el país desde donde se generó tal *wallet.*
No obstante, lo que siempre tendremos es el histórico de transacciones. Y eso nos entrega una gran ventaja, desarrollada a continuación.

4.3. Mantener registro de wallets y transacciones vinculadas a ciberdelitos

Como se mencionó previamente, siempre podremos disponer del historial de transacciones. Con lo cual, no veremos a quien corresponden los movimientos pero sí sabremos cuál es la secuencia de envío de los activos. Esto puede parecer irrelevante pero lo que hay que recordar es que las criptomonedas no tienen un valor intrínseco. Tarde o temprano deberían ser intercambiadas por bienes o servicios, provistos por entidades reales. Esta es la ventaja que da este esquema. Es muy difícil para el delincuente hacer uso anónimo de los activos cuando su histórico de transacciones es plenamente visible.
Llevado a un ejemplo claro, un delincuente no podría jamás comprar un inmueble con dinero sustraído a través de un fraude, ya que en el momento que envíe los cripto-activos, la justicia podría pedirle al vendedor que le brinde datos acerca del comprador. En un caso normal, la *wallet* del vendedor estaría pública, puesto que a él le interesa vender y no tiene por qué ocultarla.

En conclusión, no es tan fácil utilizar los activos cuando son obtenidos a través de una actividad ilícita. Esto es una diferencia positiva sobre el sistema tradicional, donde las transacciones “en negro” eluden a la justicia frecuentemente.

4.4. Estudiar la secuencia de las transacciones

Cuando los activos son obtenidos en base a una actividad ilícita, el delincuente teme que la billetera virtual esté siendo observada. Para evitar ser rastreado suele transferir el monto a otras cuentas. En este punto, el beneficio que le otorga el sistema de criptomonedas es que puede abrir tantas como quiera. Con lo cual, lo que hace son numerosos envíos a distintas cuentas que ya están bajo su dominio.
Suele ocurrir que dichos envíos siguen un patrón. Y este patrón es de un envío único por la totalidad del monto hacia otra billetera. Es una especie de concatenación de transacciones simples cuya secuencia es poco común en este tipo de sistemas. Habitualmente, el monto enviado proviene de un conjunto de transacciones entrantes y no de solo una. Es este tipo de comportamientos al que debe prestar atención el investigador. Si algo es poco común, puede tener un propósito específico. En este caso es despistarlo.
En este contexto, el delincuente suele pensar que concatenando un número significativo de estos envíos podría confundir al investigador. Pero si este último lleva un buen registro de los movimientos realizados a partir de la primera billetera involucrada, es posible que aún identifique un movimiento efectuado por el ciber-delincuente.
Para ello existen ciertos sitios que efectúan un análisis de la Blockchain y generan una representación gráfica interactiva que permite observar la secuencia y concatenación de las transacciones. Uno de ellos es https://oxt.me/
Una captura ilustrativa de su funcionalidad se muestra en la Fig. 1.

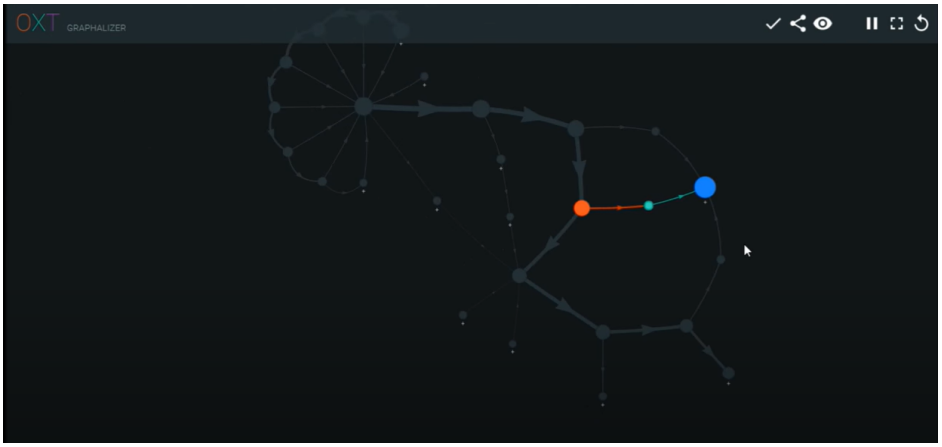

Fig. 1. Representación gráfica de la concatenación de transacciones para una billetera virtual, generada por el sitio Web https://oxt.me

5. Conclusiones

Investigar en esta rama requiere de al menos tres puntos fundamentales:

Actualizarse permanentemente en el marco jurídico que le concierne. Es un ámbito nuevo para la justicia, y su carácter tecnológico exige que las regulaciones sigan un ritmo de crecimiento vertiginoso en cuanto a la cantidad de aspectos a considerar. No es fácil adaptar tan rápidamente las disposiciones legales, para equiparar el ritmo de cambio de esta tecnología. Ergo, siempre habrá vacíos legales que serán aprovechados por cyber-delincuentes, cuestión para la cual deberá estar preparado el investigador.

Tener un contundente dominio en los conceptos tecnológicos base. Como se mencionó, esta tecnología trae tanto complicaciones como ventajas para el investigador judicial. Entonces, es de vital importancia que saque provecho de sus beneficios. Pero solo podrá hacerlo si conoce los conceptos base de su funcionamiento, a nivel técnico. Esto le permitirá saber qué tanta información puede obtener del sistema, y cómo hacerlo.
Por ejemplo, saber que toda transacción es visible, hasta en un nodo fuera de línea, y que por ello, toda secuencia que exista entre ellas también lo es.
Otro ejemplo es entender que en este sistema no existen limitaciones geográficas ni jurisdiccionales. Cualquier individuo desde cualquier lugar del mundo podría operar, independientemente de la normativa del lugar físico en el que se encuentre.

Investigar en nuevas herramientas asiduamente. A pesar de que las criptomonedas ya tienen más de una década desde su aparición, el potencial de crecimiento es aún interminable, en un futuro visible. No solo respecto a la cantidad de servicios que se pueden dar con ellas, sino a la de las herramientas de análisis que pueden surgir.
Sabemos que la información histórica de transacciones está disponible. Con lo cual, todo tipo de procesamiento imaginable es implementable. Tarde o temprano alguien lo hará. Entonces, es fundamental estar al corriente de estas nuevas soluciones, que aparecen día a día, ya que de otro modo se estarían desaprovechando los beneficios que ellas entregan.
Ejemplo, https://www.chainalysis.com/ es un sitio web, relativamente reciente que permite que los bancos, las empresas y los gobiernos tengan una comprensión de cómo las personas usan las criptomonedas.

6. Referencias

1. SAMUELSON, P. y NORDHAUS, W. (2006). Economía. (18o ed.). México: McGraw Hill. pp. 30 y 491.
2. Boar, Andrei: “Descubriendo el Bitcoin” - Ed. Profit - 2018
3. Oxt Homepage, https://oxt.me, último acceso 2021/06/06

4. Bitcoin Homepage, https://bitcoin.org/, último acceso 2021/06/06
5. Bitcoin Abuse Database Homepage, https://www.bitcoinabuse.com/, último acceso 2021/08/26
6. Wallet Explorer homepage, https://www.walletexplorer.com/, último acceso 2021/08/26
7. Bitcoin Wiki, https://en.bitcoin.it/wiki/Main_Page, último acceso 2021/08/26
8. Conrad Barski y Chris Wilmer (2015). "Bitcoin for the Befuddled". ISBN-10: 1-59327-573-0. ISBN-13: 978-1-59327-573-0. No Starch Press, Inc. 245 8th Street, San Francisco, CA 94103. info@nostarch.com. www.nostarch.com
9. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller y Steven Goldfeder. (Feb 9, 2016). "Bitcoin and Cryptocurrency Technologies". Prensa de la Universidad de Princeton, en 2016.