

**MONEDAS VIRTUALES – DEFINICIONES CLAVES Y
RIESGOS POTENCIALES DE LA/FT**

ACRÓNIMOS

ALA/CFT	Anti-Lavado de Activos / Contra la Financiación del Terrorismo
BCE	Banco Central Europeo
GAFI	Grupo de Acción Financiera
NPPS	Guía sobre el enfoque basado en el riesgo para Tarjetas Prepagas, Pagos Móviles y Pagos por Internet. (NPPS, por sus siglas en inglés).

MONEDAS VIRTUALES – DEFINICIONES CLAVES Y RIESGOS POTENCIALES DE LA/FT¹

INTRODUCCIÓN

Las monedas virtuales descentralizadas matemáticamente fundamentadas—especialmente Bitcoin²—han ido ganando cada vez más atención; han surgido dos tendencias argumentativas populares al respecto: (1) las monedas virtuales son el futuro de los sistemas de pago; y (2) las monedas virtuales proporcionan una nueva y poderosa herramienta para que criminales, financiadores del terrorismo y otros evasores de sanciones puedan mover y almacenar fondos ilícitos, fuera del alcance de las fuerzas del orden y otras autoridades.³ En este contexto, este documento se basa en la Guía sobre Nuevos Productos y Servicios de Pago (NPPS, por sus siglas en inglés) (GAFI, 2013) sugiriendo un marco conceptual para comprender y hacer frente a los riesgos de LA/FT asociados con un tipo de sistema de pago basado en Internet: las monedas virtuales. En concreto, el documento propone un compendio de definiciones comunes que clarifique qué es moneda virtual y que clasifique los diferentes tipos de moneda virtual en función de sus diferentes modelos de negocio y métodos de operación,⁴ e identifique a los participantes en los sistemas típicos de moneda virtual. También se aplican los factores de riesgo establecidos en la Sección IV (A) de la Guía de 2013 sobre NPPS a tipos específicos de monedas virtuales para identificar riesgos potenciales; del mismo modo se describen algunas investigaciones y esfuerzos recientes llevados a cabo por las fuerzas del orden en relación a casos donde se vieron involucradas monedas virtuales.

Mientras que la Guía sobre NPPS de 2013 trataba ampliamente los servicios de pago por Internet, no definía “moneda digital,” “moneda virtual,” o “dinero electrónico.” Tampoco se centraba en las monedas virtuales como un elemento distinto a los sistemas de pago basados en Internet que facilitan transacciones en dinero real (dinero fiduciario o moneda nacional) (por ejemplo, Pay-Pal, Alipay, o Google Checkout). De igual modo no se hacía referencia a las monedas virtuales convertibles descentralizadas, como Bitcoin. La Guía de 2013 señalaba también que, “[d]ada la naturaleza en desarrollo de las monedas alternativas en línea, el GAFI puede considerar seguir trabajando en este ámbito en el futuro” (Guía sobre NPPS 2013, p. 11, párr. 29). A este respecto se inició un proyecto a corto plazo sobre tipología con los siguientes objetivos:

- Desarrollar una matriz de riesgo para monedas virtuales (o quizás, más ampliamente, para monedas virtuales y dinero electrónico).
- Promover un mayor entendimiento de las partes involucradas en el sistema de monedas virtuales y la forma en que las monedas virtuales pueden ser usadas para operar sistemas de pago; y
- Alentar una discusión sobre la implementación de regulaciones ALA/CFT basadas en el riesgo en este área.

Este proyecto de tipologías podría ir más allá y derivar en un trabajo sobre políticas como la creación de una guía suplementaria para aplicar un enfoque basado en el riesgo a las monedas virtuales que podría incorporar el vocabulario propuesto, la matriz de riesgo desarrollado por el proyecto de tipologías, y explicar cómo se aplican las Recomendaciones del GAFI específicas en el contexto de monedas virtuales.

DEFINICIONES CLAVES:

Un conjunto común de términos que reflejen cómo operan las monedas virtuales es un primer paso esencial para que los funcionarios del gobierno, las agencias de aplicación de la ley, y las entidades del sector privado puedan analizar los riesgos potenciales de LA/FT de las monedas virtuales como nuevo método de pago. Como reguladores y agentes del orden público de todo el mundo empiezan a lidiar con los desafíos que presentan las monedas virtuales, se ha hecho evidente que carecemos de un vocabulario común que refleje con precisión las diferentes formas que las monedas virtuales pueden tomar. El siguiente conjunto de términos pretende fomentar el debate entre los miembros del GAFI. Es importante tener en cuenta que este vocabulario puede cambiar a medida que las monedas virtuales evolucionan y que los reguladores, las agencias de aplicación de la ley, y los funcionarios del gobierno sigan considerando los desafíos que las monedas virtuales presenten. No obstante, el vocabulario propuesto tiene como objetivo proporcionar un lenguaje común para el desarrollo de herramientas conceptuales para ayudarnos a comprender mejor cómo funcionan las monedas virtuales, y los riesgos y beneficios potenciales que comprenden.

MONEDA VIRTUAL

Moneda virtual es una representación digital⁵ de valor que puede ser comerciada digitalmente y funciona como (1) un medio de cambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero no tiene curso legal (es decir, cuando se ofrece a un acreedor, es una oferta válida y legal de pago)⁶ en ninguna jurisdicción.⁷ Ninguna jurisdicción emite o garantiza las monedas virtuales, y cumple con las funciones antes mencionadas por común acuerdo de la comunidad de sus usuarios. La moneda virtual se distingue del **dinero fiduciario** (también conocido como “**moneda real**”, “**dinero real**” o “**moneda nacional**”), porque éste funciona como la moneda y el papel moneda de un país designado como dinero de curso legal, que circula, se utiliza y acepta como medio de intercambio en el país emisor. Es diferente del **dinero electrónico** puesto que éste es una representación digital del dinero fiduciario usado electrónicamente para transferir el valor denominado en dinero fiduciario. El dinero electrónico funciona como un mecanismo de transferencia digital para el dinero fiduciario, es decir, transfiere electrónicamente un valor que tiene la condición de moneda de curso legal.

Moneda digital puede hacer referencia a una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario) y por ello a menudo su uso es intercambiable con el término “moneda virtual”. Para evitar confusión en este documento, sólo se usan los términos “moneda virtual” o “dinero electrónico.”

MONEDA VIRTUAL CONVERTIBLE VERSUS NO CONVERTIBLE

Este documento propone dividir las monedas virtuales en dos tipos básicos: moneda virtual convertible y no convertible.⁸ Aunque el documento utiliza como sinónimos “no convertible” y “cerrada”, y “convertible” y “abierta”, debe hacerse énfasis en que la noción de “moneda convertible” no implica en ningún caso la convertibilidad ex officio (por ejemplo en el caso del patrón oro), sino más bien una convertibilidad de facto (por ejemplo, por el hecho de que un mercado exista). Por ello, una moneda virtual es “convertible” siempre y cuando participantes privados las oferten y otros las acepten, ya que la “convertibilidad” no está garantizada en absoluto por ley.

Moneda virtual convertible (o abierta) tiene un valor equivalente en moneda real y puede ser intercambiada una y otra vez por dinero real.⁹ Algunos ejemplos incluyen: Bitcoin, e-Gold (fuera de uso), Liberty Reserve (fuera de uso), Second Life Linden Dollars, y WebMoney.¹⁰

Moneda virtual no convertible (o cerrada) pretende ser específica de un dominio o mundo virtual particular, como los videojuegos de rol multijugador excepcionales en línea (MMORPG, por sus siglas en inglés), o Amazon.com, y en virtud de las normas que regulan su uso, no se puede cambiar por dinero real. Algunos ejemplos incluyen: Project Entropia Dollars, Q Coins, y World of Warcraft Gold.

Cabe señalar que, aunque en virtud de los términos establecidos por el administrador una moneda no convertible sólo puede ser transferida oficialmente dentro de un entorno virtual específico y aunque en ningún caso pueda ser convertible, es posible que pueda surgir un mercado negro secundario no oficial que proporcione una oportunidad de intercambiar la moneda virtual “no convertible” por moneda fiduciaria u otra moneda virtual. Por lo general, el administrador aplicará sanciones (incluyendo la terminación de la membresía y/o confiscación de las restantes monedas virtuales) a aquellos que busquen crear o utilizar un mercado secundario en contra de las reglas de la moneda.¹¹ El desarrollo de un mercado negro secundario robusto de una moneda virtual “no convertible” puede, de hecho, transformarla en una moneda virtual convertible. Por tanto, el hecho de ser no convertible no significa que sea necesariamente estática.

MONEDAS VIRTUALES CENTRALIZADAS VERSUS DESCENTRALIZADAS

Todas las monedas virtuales no convertibles son centralizadas: por definición, son emitidas por una autoridad central que establece normas que las hacen no convertibles. Por el contrario, las monedas virtuales convertibles pueden ser cualquiera de los dos sub-tipos: centralizadas o descentralizadas.

Las **Monedas Virtuales Centralizadas** tienen una autoridad administrativa única (administrador), es decir, una tercera parte¹² que controla el sistema. Un administrador emite la moneda, establece las normas para su utilización, mantiene un libro de contabilidad central de pago, y tiene autoridad para canjear la moneda (retirla de la circulación). La tasa de cambio de una moneda virtual convertible puede ser variable, es decir, determinada por la oferta y la demanda de la moneda virtual, o fija, es decir, fijada por el administrador según un valor establecido medido en dinero real o cualquier reserva de valor del mundo real, como el oro o una cesta de divisas. En la actualidad, la gran mayoría de las

transacciones de pago en moneda virtual implican monedas virtuales centralizadas, por ejemplo: E-gold (fuera de uso), Liberty Reserve dollars/euros (fuera de uso), Second Life "Linden dollars", PerfectMoney, WebMoney "WM units", y World of Warcraft gold.

Las **Monedas Virtuales Descentralizadas (también conocidas como criptomonedas)** son monedas virtuales de código abierto fundamentadas matemáticamente que funcionan en una red de pares distribuida,¹³ sin autoridad central administradora, de vigilancia o de supervisión. Por ejemplos: Bitcoin, Litecoin y Ripple.¹⁴

La **Criptomoneda** se refiere a una moneda virtual convertible descentralizada fundamentada matemáticamente y que está protegida por criptografía, es decir, que incorpora los principios de la criptografía para implementar una economía de la información segura, descentralizada y distribuida. Las criptomonedas se basan en llaves públicas y privadas para transferir el valor de una persona (individuo o entidad) a otra, y debe ser criptográficamente firmado cada vez que se transfiere. La seguridad, la integridad y la armonía de los libros de contabilidad de la criptomoneda están garantizadas por una red de partes mutuamente desconfiadas (en Bitcoin se conocen como mineros) que protegen la red a cambio de la obtención de una tasa distribuida aleatoriamente (en Bitcoin, un pequeño número de nuevas unidades de bitcoins llamado "recompensa de bloque" y en algunos casos, también las tasas por transacción que pagan los usuarios como incentivo para que los mineros incluyan sus transacciones en el próximo bloque). Se han definido decenas de especificaciones sobre las criptomonedas; la mayoría se derivan de Bitcoin, y utilizan un sistema de prueba de trabajo para validar las transacciones y mantener la cadena de bloques. Si bien Bitcoin significó la primera implementación del protocolo de una criptomoneda, hay un creciente interés en el desarrollo de métodos de prueba alternativos y potencialmente más eficientes, como los sistemas basados en la prueba de participación.

Bitcoin, lanzado en 2009, fue la primera moneda virtual convertible descentralizada, y la primera criptomoneda. Los bitcoins son unidades de cuenta compuestos de secuencias alfanuméricas únicas que constituyen unidades de moneda y que tienen valor sólo porque usuarios individuales están dispuestos a pagar por ellos. Los bitcoins se comercian digitalmente entre los usuarios contando con un alto grado de anonimato y se pueden cambiar (comprar o canjear) por dólares estadounidenses, euros y otras monedas fiduciarias o virtuales. Cualquier persona puede descargar el software gratuito de código abierto de un sitio Web para enviar, recibir y almacenar bitcoins, así como para monitorear las transacciones de bitcoins. Los usuarios también pueden obtener direcciones de Bitcoin, que funcionan como cuentas, en un intercambiador de Bitcoin o servicio de monedero en línea. Las transacciones (flujos de fondos) están públicamente disponibles en un registro de transacciones compartidas e identificadas por la dirección Bitcoin, una secuencia alfanumérica que no está sistemáticamente conectada a un individuo. Por ello, se dice que Bitcoin es "pseudo-anónimo". Bitcoin tiene un tope de 21 millones de unidades (pero cada unidad puede dividirse en unidades más pequeñas), proyectadas a alcanzarse en 2140¹⁵. A fecha de abril de 2014, había casi 12 millones y medio de bitcoins, con un valor total de poco más de U\$D 5.5 mil millones, de acuerdo al promedio de la tasa de cambio de dicha fecha.

Altcoin es cualquier moneda virtual convertible descentralizada fundamentada matemáticamente distinta al Bitcoin—la original. Algunos ejemplos actuales son: Ripple, PeerCoin, Lite-coin, zerocoin,

anoncoin y dogecoin. Según consta, a fecha de 2 de abril de 2014, un intercambiador popular (Cryptsy) intercambiaba más de 100 monedas virtuales diferentes (Popper, N., 2013).

Programas de Anonimato (Herramienta de Anonimato) se refiere a las herramientas y servicios, tales como redes oscuras y mezcladores, diseñados para ocultar el origen de una transacción Bitcoin y facilitar el anonimato. (Ejemplos: Tor (red oscura), Monedero Oscuro (red oscura), Lavandería Bitcoin (mezclador)).

Mezclador (Servicio de Lavandería, Conmutador) es un tipo de programa de anonimato que oscurece la cadena de transacciones en la cadena de bloques vinculando todas las transacciones a la misma dirección Bitcoin y enviándolas juntas de una manera que parezca que hubieran sido enviadas desde otra dirección. Un mezclador o conmutador envía transacciones a través de una serie compleja y semi-aleatoria de transacciones ficticias que hace que sea extremadamente difícil la vinculación de monedas virtuales específicas (direcciones) con una transacción en particular. Los servicios de mezcladores operan cuando reciben instrucciones de un usuario para enviar fondos a una dirección Bitcoin en particular. El servicio de mezcla “combina” esta transacción con otras transacciones del usuario, de tal manera que deja poco claro el destinatario de la transferencia que el usuario intenta hacer. (Ejemplos: Bitmixer.io, SharedCoin, Blockchain.info, Bitcoin Laundry, Bitlaunder, Easycoin).

Tor (originalmente, The Onion Router) es una red distribuida clandestina de computadoras en Internet que oculta las direcciones IP verdaderas, y por lo tanto las identidades de los usuarios de la red, mediante el enrutamiento de comunicaciones/transacciones a través de múltiples ordenadores en todo el mundo y envolviéndolos en numerosas capas de cifrado. Tor hace que sea muy difícil localizar físicamente las computadoras que alojan o acceden a sitios web en la red. Esta dificultad puede ser exacerbada por el uso de conmutadores o programas de anonimato adicionales en la red Tor. Tor es una de varias redes de computadoras distribuidas clandestinamente, a menudo referida como red oscura, cypherspace, Web Profunda, o redes anónimas, y que son utilizadas por personas para acceder a contenidos de una manera diseñada para ocultar su identidad y la actividad asociada a ellos en Internet.

Monedero Oscuro es un monedero virtual dentro del navegador, disponible en Chrome (y potencialmente en Firefox), que busca garantizar el anonimato de las transacciones Bitcoin mediante la incorporación de las siguientes características: auto-anonimato (mezclador), comercialización descentralizada, plataformas incensurables de micromecenazgo, plataformas de valores e información de mercados negros, y sitios de mercados descentralizados similares a la Ruta de la Seda.

Almacenamiento en frío se refiere a una billetera Bitcoin off-line, es decir, una billetera Bitcoin que no está conectada a Internet. El almacenamiento en frío está destinado a ayudar a proteger de la piratería y el robo la moneda virtual almacenada.

Almacenamiento en caliente se refiere a una billetera Bitcoin on-line. Debido a que está conectado a Internet, el almacenamiento en caliente es más vulnerable a la piratería/robo que el almacenamiento en frío.

Sistema de Cambio Local (LETS, por sus siglas en inglés) es una organización económica organizada a nivel local que permite a sus miembros intercambiar bienes y servicios con el resto del grupo. LETS usa una moneda creada localmente para denominar unidades de valor que pueden ser objeto de comercio o intercambio a cambio de bienes o servicios. Teóricamente, los bitcoins podrían ser adoptados como moneda local utilizada dentro de un LETS. (Ejemplos: Ithica Dollars o Mazacoin).

PARTICIPANTES EN EL SISTEMA DE MONEDA VIRTUAL

Un **intercambiador (también llamado a veces servicio de intercambio de moneda virtual)** es una persona o entidad que ejerce una actividad en el intercambio de moneda virtual por dinero real, fondos, u otras formas de moneda virtual, así como metales preciosos, y viceversa, a cambio de una tasa (comisión). Los intercambiadores generalmente aceptan una amplia gama de pagos, incluyendo dinero en efectivo, giros, tarjetas de crédito, y otras monedas virtuales, y pueden estar afiliados al administrador o no afiliados, o ser un proveedor externo. Los intercambiadores pueden funcionar como bolsa u oficina de cambio. Las personas suelen utilizar intercambiadores para depositar y retirar dinero de cuentas en moneda virtual.

Un **administrador** es una persona o entidad involucrada en el proceso de emisión (puesta en circulación) de una moneda virtual centralizada, estableciendo las normas para su uso, manteniendo un libro de contabilidad central de pago, y disponiendo de la autoridad para canjear (retirar de la circulación) la moneda virtual.

Un **usuario** es una persona/entidad que obtiene dinero virtual y lo utiliza para comprar bienes o servicios reales o virtuales, enviar transferencias en su capacidad personal a otra persona (para uso personal), o que mantiene la moneda virtual como una inversión (personal). Los usuarios pueden obtener la moneda virtual de varias maneras. Por ejemplo, (1) pueden comprar moneda virtual usando dinero real (en un intercambiador o en el caso de algunas monedas virtuales centralizadas directamente al administrador/emisor); (2) pueden participar en actividades específicas a través de las cuales perciben pagos en moneda virtual (por ejemplo, responder a una promoción, completar una encuesta en línea, proporcionar un bien o un servicio real o virtual); (3) con algunas monedas virtuales descentralizadas (por ejemplo Bitcoin), a través de la auto-generación de unidades de moneda mediante la "minería" (ver definición de minero más abajo), y recibéndolas como regalo, como recompensa, o como parte de una distribución inicial gratuita.

Un **minero** es una persona o entidad que participa en una red de moneda virtual descentralizada mediante la ejecución de un software especial para resolver complejos algoritmos en una prueba de trabajo distribuida u otro sistema de prueba distribuido utilizado para validar las transacciones en el sistema de moneda virtual. Los mineros pueden ser usuarios, si se autogeneran una moneda virtual convertible únicamente para sus propios fines, por ejemplo, para mantener la inversión, para pagar una obligación existente o para comprar bienes y servicios. Los mineros también pueden participar en un sistema de moneda virtual como intercambiadores, generando moneda virtual como un negocio con el fin de venderla por moneda fiduciaria u otra moneda virtual.

Billetera virtual es un medio (aplicación de software u otro mecanismo/medio) para guardar, almacenar y transferir bitcoins u otra moneda virtual.

Un proveedor de billetera es una entidad que ofrece una billetera de dinero virtual (es decir, un medio (aplicación de software u otro mecanismo/medio) para guardar, almacenar y transferir bitcoins u otra moneda virtual). Una billetera contiene las llaves privadas del usuario que permiten al usuario gastar moneda virtual asignada a la dirección de moneda virtual en la cadena de bloque. Un proveedor de billetera facilita la participación en un sistema de moneda virtual permitiendo a los usuarios, intercambiadores y comerciantes llevar a cabo más fácilmente las transacciones en monedas virtuales. El proveedor de billetera mantiene el saldo de la moneda virtual del cliente y, generalmente, ofrece almacenamiento y seguridad en transacciones. Por ejemplo, más allá de proporcionar direcciones de bitcoins, la billetera puede ofrecer encriptación, protección de firma mediante múltiples llaves (multi-llaves), copia de seguridad/almacenamiento en frío, y mezcladores. Todas las billeteras Bitcoin pueden interoperar entre sí. Las billeteras pueden almacenarse tanto on-line ("almacenamiento en caliente") como off-line ("almacenamiento en frío"). (Ejemplos: Coinbase, Multibit, o Bitcoin Wallet).

Además, algunas **otras entidades** pueden participar en un sistema de moneda virtual y pueden estar afiliadas con intercambiadores y/o administradores, o ser independientes. Entre estos se incluyen los **proveedores de servicios de administración Web (también conocidos como administradores de sitios web); remitentes de pagos de terceros** que facilitan la aceptación de comerciantes; **desarrolladores de software;** y **proveedores de aplicaciones** (algunas de las "otras entidades" mencionadas en este párrafo podría encuadrarse en alguna de las categorías indicadas anteriormente). El desarrollo de aplicaciones y softwares pueden servir por un lado para propósitos legítimos, por ejemplo, para facilitar la aceptación del comerciante y los pagos del cliente, o para responder a las preocupaciones legítimas de privacidad; por otro lado también pueden servir para fines ilícitos, por ejemplo, un desarrollador u operador de un mezclador puede dirigirse a usuarios con propósitos ilícitos con productos diseñados para evitar el escrutinio de los reguladores y de las agencias de aplicación de la ley.

Hay que destacar que esta lista de participantes no es exhaustiva. Por otra parte, dado el rápido desarrollo de las tecnologías de las monedas virtuales y los modelos de negocios, podrían surgir participantes adicionales dentro de los sistemas de moneda virtual y plantear riesgos potenciales de LA/FT.

Taxonomía de las Monedas Virtuales

	Centralizada	Descentralizada
Convertible	Administrador, intercambiador, usuario, terceras partes; puede ser cambiada por dinero real. Ejemplo: WebMoney	Intercambiadores, usuarios (no administrador), terceras partes no fiables; puede ser cambiado por dinero real. Ejemplo: Bitcoin

No convertible	Administrador, intercambiador, usuario, terceras partes; no puede ser cambiada por dinero real. Ejemplo: World of Warcraft Gold	No existe
-----------------------	---	-----------

USOS LEGÍTIMOS

Al igual que otros nuevos métodos de pago, la moneda virtual tiene usos legítimos; existen destacadas empresas de capital de riesgo que invierten en moneda virtual de nueva creación. La moneda virtual tiene el potencial tanto para mejorar la eficiencia de pago, como para reducir los costos de transacción para los pagos y transferencias de fondos. Por ejemplo, Bitcoin funciona como una moneda global que puede evitar los cargos por cambio, y es actualmente procesada a tasas/cargos menores que las tarjetas de crédito y débito tradicionales, y puede potencialmente proporcionar un beneficio a los sistemas de pago en línea existentes, como Paypal.¹⁶ La moneda virtual puede facilitar los micropagos, permitiendo a los negocios monetizar en Internet bienes y servicios de muy bajo costo como juegos de una sola partida o descargas de música. Actualmente, desde un punto de vista práctico, estos productos no pueden venderse a un bajo costo apropiado por unidad debido a los altos costos de transacción asociados, por ejemplo, con pagos con tarjeta de crédito o débito. Las monedas virtuales pueden del mismo modo facilitar las remesas internacionales y promover la inclusión financiera de otras maneras, a medida que se desarrollan nuevos productos y servicios basados en monedas virtuales que puedan servir potencialmente a las personas poco bancarizadas o desbancarizadas. Las monedas virtual—en particular Bitcoin—pueden también mantenerse con la finalidad de servir como inversión. Estos beneficios potenciales deben ser analizados cuidadosamente, incluyendo si se mantendrán las ventajas en costos si la moneda virtual quedase sujeta a requisitos regulatorios similares a los que se aplican a otros métodos de pago, y/o si estarán incluidas las tasas de cambio para hacer un retiro en moneda fiduciaria, y si la volatilidad, la protección del consumidor y otros factores¹⁷ limitan su potencial en términos de inclusión financiera.

RIESGOS POTENCIALES

Las monedas virtuales convertibles que pueden ser canjeadas por dinero real o por otras monedas virtuales son potencialmente vulnerables a abusos por lavado de dinero y financiación del terrorismo por muchos de los motivos señalados en la guía de NPPS de 2013. En primer lugar, pueden permitir mayor anonimato que los métodos de pago tradicionales que no usan dinero en efectivo. Las monedas virtuales pueden ser intercambiadas en Internet, y se caracterizan generalmente por las relaciones entre clientes no presenciales y por permitir la financiación anónima (uso de efectivo o de terceros a través de intercambiadores virtuales que no identifiquen correctamente la fuente de financiación). También pueden permitir las transferencias anónimas, si el remitente y el destinatario no se identifican adecuadamente.

Los sistemas descentralizados son especialmente vulnerables a los riesgos de anonimato. Por ejemplo, por diseño, las direcciones Bitcoin que funcionan como cuentas no tienen nombres ni otra identificación

del cliente, además el sistema no tiene ningún servidor o proveedor de servicios central. El protocolo de Bitcoin ni requiere, ni proporciona la identificación y verificación de los participante, tampoco genera registros del historial de transacciones asociadas a identidades del mundo real. No hay ningún órgano de control central, y o software anti-lavado de activos para monitorear e identificar transacciones sospechosas. Las fuerzas del orden no puede identificar una ubicación central o entidad (administrador) para fines investigativos o de embargo de activos (aunque las autoridades pueden dirigirse a intercambiadores individuales para conseguir información de clientes que puedan tener). Por lo tanto, esto ofrece un nivel potencial de anonimato que se ha probado imposible con otros métodos de pago como tarjetas de crédito y débito tradicionales o sistemas de pago en línea más antiguos, como PayPal.

El alcance global de la moneda virtual hace que se incremente de igual forma sus riesgos potenciales de LA/FT. Se pueden acceder a los sistemas de moneda virtual a través de Internet (incluyendo los teléfonos celulares) y se pueden utilizar para hacer pagos transfronterizos y transferencias de fondos. Además, las monedas virtuales se basan por lo general en infraestructuras complejas que involucran a varias entidades, a menudo repartidas en varios países, para transferir fondos o ejecutar pagos. Esta segmentación de los servicios implica que la responsabilidad de cumplimiento de la normativa anti-lavado de activo y contra la financiación del terrorismo, así como la supervisión quede poco clara. Por otra parte, los registros de clientes y de transacciones pueden ser mantenidos por distintas entidades, a menudo en diferentes jurisdicciones, lo que hace más difícil que las fuerzas del orden y los reguladores puedan tener acceso a ellos. Este problema se ve agravado por la rápida evolución de la tecnología de las monedas virtuales descentralizadas y de los modelos de negocio, incluido el número cambiante y los tipos/roles de los participantes que prestan servicios en los sistemas de pagos en moneda virtual. Es importante destacar que los componentes de un sistema de moneda virtual pueden estar ubicados en jurisdicciones que no cuenten con adecuados controles ALA/CFT. Los sistemas de monedas virtuales centralizados podrían ser cómplices de lavado de dinero y deliberadamente podrían buscar jurisdicciones con regímenes ALA/CFT débiles. Las monedas virtuales convertibles descentralizadas que permiten transacciones anónimas de persona a persona pueden parecer existir en un universo digital totalmente fuera del alcance de cualquier país en particular.

ACCIONES LEGALES QUE IMPLICAN MONEDA VIRTUAL

Las fuerzas del orden ya están identificando casos que involucran el abuso de monedas virtuales para lavar dinero. Algunos ejemplos incluyen:

LIBERTY RESERVE

Hasta la fecha ha sido el mayor caso de lavado de dinero en línea de la historia. En mayo de 2013, el Departamento de Justicia de EE.UU. acusó a Liberty Reserve, un transmisor de dinero con sede en Costa Rica, y siete de sus directivos y empleados por operar un negocio de transferencia de dinero no registrado y de lavado de dinero para facilitar el movimiento de más de USD 6 mil millones en ganancias ilícitas. En una acción coordinada, el Departamento del Tesoro identificó Liberty Reserve

como una institución financiera de riesgo en materia de lavado de activos según la Sección 311 del USA PATRIOT Act. Finalmente, la empresa fue cesada del sistema financiero de EE.UU.

Establecida en 2006, Liberty Reserve fue diseñada para evitar el escrutinio regulatorio y de cumplimiento de la ley, y para ayudar a los criminales a distribuir, almacenar y blanquear el producto del fraude de tarjetas de crédito, robo de identidad, fraude de inversiones, piratería informática, tráfico de narcóticos y pornografía infantil, ya que permitía la realización de transacciones financieras anónimas y no rastreables. Operando a una escala enorme, tenía más de un millón de usuarios en todo el mundo, incluyendo más de 200.000 en los Estados Unidos, y manejaba aproximadamente 55 millones de transacciones, casi todas las cuales eran ilegales. Tenía su propia moneda virtual, Liberty Dollars (LR), pero en el paso final del proceso de las operaciones, las transferencias estaban denominadas y almacenadas en dinero real (dólares estadounidenses).

Para utilizar la moneda LR, un usuario abría una cuenta a través de la página Web de Liberty Reserve. A pesar de que Liberty Reserve requería ostensiblemente la información básica de identificación, no validaba luego las identidades. Los usuarios establecían rutinariamente cuentas bajo nombres falsos, incluyendo nombres descaradamente criminales ("Russia Hackers", "Hacker Account", "Joe Bogus") y direcciones descaradamente falsas ("Fake 123 Main Street, Completely Made Up City, Nueva York"). Para agregar una capa adicional de anonimato, Liberty Reserve requería que los usuarios hicieran depósitos y retiros a través de terceros intercambiadores recomendados—generalmente empresas transmisoras de dinero sin licencia que operan en Rusia y en varios países con una débil supervisión y regulación gubernamental en materia de lavado de dinero hasta ese momento, como el caso de Malasia, Nigeria y Vietnam. Al evitar los depósitos directos y retiros de los usuarios, Liberty Reserve evadía la recopilación de información sobre ellos a través de transacciones bancarias o cualquier otra actividad que pudiera crear un registro. Una vez establecida una cuenta, un usuario podía realizar transacciones con otros usuarios de Liberty Reserve transfiriendo LR desde su cuenta a la de los otros usuarios, incluidos "mercaderes" de sociedades pantallas que aceptasen LR como pago. Por una "cuota de privacidad" extra (75 centavos de dólar por transacción), los usuarios podían ocultar sus números de cuenta de Liberty Reserve al transferir fondos, haciendo que las transferencias fueran completamente imposible de rastrear. Después de enterarse de que estaba siendo investigada por las fuerzas del orden de los EE.UU., Liberty Reserve fingió cerrar en Costa Rica, pero continuó operando a través de un conjunto de empresas ficticias, moviendo millones a través de sus cuentas en Australia, Chipre, China, Hong Kong, Marruecos, Rusia, España, y otros lugares.¹⁸

SILK ROAD (Ruta de la Seda)

En septiembre de 2013, el Departamento de Justicia de EE.UU. inició una denuncia criminal acusando al supuesto propietario y operador de la Ruta de la Seda, un sitio oculto diseñado para permitir a sus usuarios comprar y vender drogas ilegales, armas, información de identidades robadas, y otros bienes y servicios ilegales de forma anónima y fuera del alcance de las fuerzas del orden, donde se manejaban conspiraciones de tráfico de drogas, piratería informática y lavado de dinero. El Departamento de Justicia también se apoderó de la página Web y de aproximadamente 173.991 bitcoins de equipos informáticos incautados por un valor de más de USD 33.6 millones en el momento de la incautación. El

acusado fue detenido en San Francisco en octubre y acusado en febrero de 2014; la investigación está en curso.

Lanzada en enero de 2011, la Ruta de la Seda funcionaba como un bazar global de mercado negro cibernético que mediaba en las transacciones criminales anónimas y era utilizada por varios miles de traficantes de drogas y otros vendedores ilegales para distribuir bienes y servicios ilegales a más de cien mil compradores, un tercio de los cuales se cree que han estado en los Estados Unidos. Supuestamente generó ingresos totales por ventas de aproximadamente U\$D 1,2 mil millones de dólares (más de 9,5 millones de bitcoins) y aproximadamente U\$D 80 millones (más de 600.000 bitcoins) en comisiones para la Ruta de la Seda. Cientos de millones de dólares fueron lavados a través de estas transacciones (tomando como referencia el valor del bitcoin en la fecha de incautación). Las comisiones oscilaban entre el 8 y el 15 por ciento del precio de venta total.

La Ruta de la Seda disfrutaba de anonimato operando en la red Tor oculta y aceptando sólo bitcoins como medio de pago. Usando bitcoins como moneda exclusiva la Ruta de la Seda permitía a los compradores y vendedores ocultar aún más su identidad, ya que los remitentes y destinatarios de transacciones de bitcoins entre pares (P2P) se identificaban sólo por la dirección/cuenta anónima de bitcoin. Por otra parte, los usuarios podían obtener un número ilimitado de direcciones de bitcoin y utilizar una diferente para cada transacción, oscureciendo aún más el rastro de ganancias ilícitas. Los usuarios también podían utilizar "programas de anonimato" adicionales, más allá del servicio de mezcladores/conmutadores integrado en las transacciones de la Ruta de la Seda (véase más adelante).

El sistema de pagos de la Ruta de la Seda funcionaba como un banco interno de Bitcoin, donde cada usuario tenía que tener una cuenta con el fin de llevar a cabo transacciones en el sitio. Cada usuario tenía al menos una dirección de Bitcoin de la Ruta de la Seda (y potencialmente miles) asociadas con la cuenta de la Ruta de la Seda del usuario, almacenada en billeteras mantenidas en servidores controlados por la Ruta de la Seda. Para realizar una compra, el usuario obtenía bitcoins (normalmente a través de un intercambiador de bitcoins) y los enviaba a una dirección Bitcoin asociada con su cuenta de la Ruta de la Seda para financiar la cuenta. Cuando se hacía una compra, la Ruta de la Seda transfería los bitcoins del usuario a una cuenta de depósito en garantía y se mantenía, en espera de la finalización de la transacción, y luego se transferían los bitcoins del usuario/comprador de la cuenta de depósito en garantía a la dirección de Bitcoins de la Ruta de la Seda del proveedor. Como un paso más, la Ruta de la Seda empleaba un "mezclador/conmutador" por cada compra que, como el sitio explica, "enví[a] todos los pagos a través de una compleja serie semi-aleatoria de transacciones ficticias ... - por lo que es casi imposible vincular el pago con cualquier [bit]coin que sale del sitio."

WESTERN EXPRESS INTERNATIONAL

Una investigación de ocho años de un grupo de la delincuencia informática multinacional con sede en Internet (Western Express Cybercrime Express), terminó en condenas o declaraciones de culpabilidad de 16 de sus miembros por su participación en un esquema global de robo/fraude cibernético de identidad. Los miembros del grupo cibercriminal interactuaron y se comunicaron principalmente a

través de Internet mediante Webs de verificación de identidad dedicadas al robo de tarjeta de crédito e información de identificación personal, y usaba identidades falsas, cuentas de mensajería instantánea anónimas, cuentas de correo electrónico anónimas, y cuentas en moneda digitales anónimas para ocultar la existencia y el propósito de la empresa criminal, evitar ser detectados por las autoridades y los organismos reguladores, y mantener su anonimato.

La empresa criminal estaba compuesta por vendedores, compradores, proveedores de servicios de delitos informáticos, y personas encargadas de mover dinero ubicadas en numerosos países, desde Ucrania y a través de Europa del Este hacia los Estados Unidos. Los vendedores vendieron casi 100.000 números de tarjetas de crédito robadas y otra información de identificación personal a través de Internet, y recibían el pago en su mayoría en e-Gold y WebMoney. Los compradores utilizaban las identidades robadas para falsificar tarjetas de crédito y comprar mercancía costosa que traficaban (incluso a través de esquemas de re- envío), cometiendo otros delitos, como robo, posesión criminal de propiedad robada, y fraude, y generando ingresos procedentes del fraude de tarjetas de crédito de alrededor de U\$D 5 millones. Los proveedores de servicios de delitos informáticos promovieron, facilitaron y ayudaron en la compra, venta y uso fraudulento de números de tarjetas de crédito robados y otra información de identificación personal por la prestación de servicios informáticos a los vendedores y los compradores. Las personas que movían dinero blanquearon ganancias ilícitas del grupo criminal usando alta tecnología, moviendo más de U\$D 35 millones a través de varias cuentas.

El centro de toda la operación era Western Express International, Inc., una corporación de Nueva York con sede en Manhattan que operaba como un intercambiador de moneda virtual y transmisor de dinero sin registrar para coordinar y facilitar los métodos de pago por Internet utilizados por la empresa criminal, y para lavar las ganancias del grupo. Una de las más grandes casas de cambio virtuales en los Estados Unidos, Western Express International intercambió un total de U\$D 15 millones en WebMoney y U\$D 20 millones en e-Gold para el grupo cibercriminal y utilizaron bancos y transmisores de dinero tradicionales para mover grandes sumas de dinero. También proporcionó información y asistencia a través de sus sitios Web (incluyendo Dengiforum.com y Paycard2000.com) sobre formas de mover dinero anónimamente y fuera del alcance de los requisitos de presentación de informes.

Western Express Internacional y su propietario/operador, un ciudadano ucraniano, se declararon culpable en febrero de 2013 en el Estado de Nueva York por lavado de dinero, fraude y delitos de conspiración. (En febrero de 2006, Western Express también fue acusado de tener una casa de cambio/servicio de transferencias ilegales.) Otros tres acusados fueron condenados tras un juicio en junio de 2013; varios declarantes también se declararon culpable en agosto de 2009. Dos acusados permanecen prófugos. La investigación fue realizada conjuntamente por el Servicio Secreto de los EE.UU. y la Oficina del Fiscal del Distrito de Manhattan (en Nueva York), y fue procesado con éxito por éste último.¹⁹

NOTAS

1. El primer borrador de este documento fue preparado conjuntamente por Australia, Canadá, Rusia, el Reino Unido y los Estados Unidos para las reuniones del GAFI en febrero de 2014. Después de dicha reunión se invitó a todas las delegaciones a formular comentarios sobre el borrador con miras a la adopción de un documento final en la próxima reunión. Se recibieron comentarios de 10 delegaciones, y éstos han sido tomados en cuenta en la preparación de esta revisión.
2. “Bitcoin” (en mayúsculas) se refiere tanto al software abierto usado para crear la moneda virtual y la red de pares (P2P) resultante; “bitcoin” (en minúsculas) se refiere a las unidades individuales de la moneda virtual.
3. Debe tenerse en cuenta que muchos observadores, entre los cuales se incluyen el ex Presidente de la Reserva Federal de los EE.UU., Alan Greenspan, y Nout Wellink, un ex Presidente del Banco Central alemán, y el Premio Nobel de Economía Robert Shiller, piensan que las monedas virtuales son una moda pasajera o una burbuja, semejante a la fiebre del Tulipán del siglo XVII en los Países Bajos.
4. La moneda virtual es un elemento complejo que no sólo implica temas de LA/FT, sino que también implica otros temas regulatorios, incluyendo la protección del consumidor, la seguridad prudencial, los impuestos y solidez regulatoria, y las normas de seguridad de redes. El vocabulario propuesto es por lo tanto relevante a través de una serie de jurisdicciones regulatorias complementarias. La adopción de términos consistentes y una comprensión conceptual común sobre moneda virtual por parte de todas las entidades gubernamentales pertinentes es importante para evitar la duplicación de esfuerzos y/o el trabajo con propósitos cruzados no deseados, y facilita la capacidad de las autoridades gubernamentales de aprovechar sus diferentes perspectivas y áreas de conocimiento con el fin de identificar y abordar con mayor eficacia los asuntos relacionados con las monedas virtuales.
5. **Representación digital** es una representación de algo en forma de dato digital, es decir, datos informáticos representados con el uso de valores (discontinuos) discretos que conforman la información, a diferencia de las señales continuas, o análogas que funcionan de manera continua o representan información utilizando una función continua. Un objeto físico, como una memoria externa o una moneda Bitcoin, puede contener una representación digital de moneda virtual, pero en última instancia, la moneda sólo funciona como tal si está conectada digitalmente, vía Internet, al sistema de moneda virtual.
6. Tener curso legal no requiere necesariamente que una entidad o individuo acepte el pago en un determinado tipo de moneda de curso legal. Por ejemplo, en muchas jurisdicciones, una empresa privada, persona, u organización es libre de desarrollar políticas internas sobre la conveniencia o no de aceptar el dinero físico o monedas (efectivo) como pago por bienes y / o servicios.
7. Esta definición difiere de la proporcionada en 2012 por el Banco Central Europeo (BCE), la cual definía moneda virtual “como un tipo de dinero digital no regulado emitido y normalmente controlado por sus desarrolladores, y usado y aceptado entre los miembros de una comunidad virtual específica” BCE, *Esquemas de Moneda Virtual* (Octubre de 2012), p.6. El BCE reconoce en la p. 13 de dicho informe que su “definición puede necesitar ser adaptada en el futuro si las características fundamentales cambiasen.” La definición del BCE parece ahora demasiado limitada, ya que las monedas virtuales descentralizadas matemáticamente fundamentadas, tales como el Bitcoin no son emitidas y controladas por un desarrollador central, y algunas jurisdicciones (Estados Unidos, Suecia, y Tailandia) ahora regulan las monedas virtuales.
8. Esta categorización difiere de la clasificación en tres partes del BCE, el cual divide las monedas virtuales en tres tipos: “Tipo 1 . . . se refiere[e] esquemas cerrados de moneda virtual . . . usados en juegos en línea. Tipo 2 . . . [se refiere a] esquemas [que] tienen un flujo unidireccional (normalmente una entrada), es decir, que hay una tasa de conversión por la compra de la moneda virtual, que puede . . . ser usada para comprar bienes o servicios virtuales . . . (y excepcionalmente también . . . bienes y servicios reales) . . . Tipo 3 [se refiere a] esquemas . . . [con] flujos bidireccionales, es decir, la moneda virtual . . . funciona como cualquier . . . moneda convertible [real], con . . . tasas de cambio [compra y venta]. . . [y] puede . . . ser usada para comprar [ambos] bienes y

servicios virtuales . . . [y] reales.” (BCE *Esquemas de Monedas Virtuales*, p. 6.). Este documento de trabajo adopta una clasificación más simple y dividida porque actualmente, sólo las monedas virtuales (totalmente) convertibles que pueden ser usadas para transferir valor dentro y fuera del sector financiero formal presentan riesgos significantes de LA/FT. Esto se debe a que el lavado de activos requiere: la conversión o transferencia (de fondos ilícitos), la ocultación o encubrimiento de la fuente/origen (de los fondos ilícitos), o la adquisición/posesión/uso (de fondos ilícitos).

9. Algunas monedas virtuales convertibles pueden ser directamente cambiadas a través del administrador que las emite (directamente cambiadas); otras deben ser cambiadas a través de intercambiadores de moneda virtual (intercambiador externo).
10. Por ejemplo, WebMoney es una moneda virtual porque (activos) “con valor” son transferidos y almacenados en forma de moneda no fiduciaria. Las unidades de medida de los derechos de propiedad de los valores almacenados por el garante son WebMoney Title Units (WM) del tipo correspondiente. <http://wmtransfer.com/eng/about/>
11. Por ejemplo, a pesar de las medidas de disuasión, varios intercambios permiten convertir World of Warcraft Gold en el mercado negro.
12. Un tercero es una persona o entidad que está involucrada en una transacción, pero no es uno de los actores principales y no está afiliado con los otros dos participantes en la transacción, es decir, un tercero funciona como una entidad neutral entre los principales actores (por ejemplo, el emisor y el receptor, el comprador y el vendedor) en un negocio o transacción financiera. La participación de un tercero varía con el tipo de negocio o transacción financiera. Por ejemplo, un portal de pago en línea, como PayPal, actúa como un tercero en una transacción de venta. Un vendedor ofrece un bien o servicio; un comprador utiliza una tarjeta de crédito o débito introducida mediante el servicio de pago de PayPal, y el tercero completa la transferencia financiera. Del mismo modo, en una transacción de bienes raíces, una empresa de depósitos en garantía externa actúa como agente neutral entre el comprador y el vendedor, encargándose de reunir los documentos por parte del vendedor y el dinero del comprador que ambos participantes principales necesitan intercambiar para completar la transacción.
13. Distribuido es un término técnico que se refiere a una característica esencial de las monedas virtuales descentralizadas matemáticamente fundamentadas: las transacciones son validadas por un sistema de prueba de trabajo *distribuido*. Cada transacción se *distribuye* entre una red de participantes que ejecutan el algoritmo para validar la transacción.
14. Además de la creación inicial y emisión de ripple coins (RXP), Ripple funciona como una moneda virtual descentralizada. Los fundadores de Ripple crearon los 100 mil millones de monedas ripple y retuvieron 20 mil millones de ellas, para ser distribuidas por una entidad independiente, Ripple Labs. Sin embargo, todas las transacciones son verificadas por una red informática descentralizada, utilizando el protocolo de código abierto de Ripple, y son registradas en un libro compartido que es una base de datos constantemente actualizada de las cuentas y transacciones Ripple.
15. En 2140, la recompensa de bloque dejará de estar disponible y los mineros serán recompensados sólo mediante tasas pagadas por cada transacción.
16. Por ejemplo, PayPal está buscando activamente aceptar bitcoins en su plataforma, y JP Morgan Chase ha presentado una solicitud de patente en EE.UU. de un sistema de pago electrónico en línea utilizando un protocolo de moneda virtual matemáticamente fundamentada que permita a los usuarios realizar pagos anónimos sin proporcionar un número de cuenta o nombre, con la moneda virtual que se almacena en las computadoras JPMC y verificado a través de un registro compartido, al igual que 'la cadena de bloques' en el sistema Bitcoin.
17. Por ejemplo, queda por ver si los sistemas de moneda virtual pueden proporcionar un camino a otros servicios financieros, como el crédito y los seguros.
18. La investigación y desmantelamiento de Liberty Reserve acarrió la acción de las fuerzas del orden de 18 países y jurisdicciones para frenar el producto del delito, decomisar los dominios, e incautar los servidores. Entre estos

países se encuentran: Costa Rica, Países Bajos, España, Marruecos, Suecia, Suiza, Chipre, Australia, China, Hong Kong, Noruega, Letonia, Luxemburgo, Reino Unido, Rusia, Canadá y los Estados Unidos.

19. La investigación de la Ruta de la Seda involucró a múltiples agencias de aplicación de la ley estadounidenses, liderada por la División Informática y de Operaciones Especiales de Nueva York de la Oficina Federal de Investigación (FBI), y el Cuerpo de Intervención contra el Crimen Organizado relacionado con las Drogas de Nueva York de la Administración del Control de Drogas (DEA) (compuesta por agentes y oficiales de la DEA, del Servicio de Rentas Internas (IRS), el Departamento de Policía de la Ciudad de Nueva York, Migraciones y Aduanas (ICE), Investigaciones de Seguridad Nacional (HSI), la Policía Estatal de Nueva York, la Oficina de Alcohol, Tabaco, Armas y Explosivos, los Servicios Secretos estadounidenses, el Servicio de Mariscales de Estados Unidos, la Oficina de Control de Activos Extranjeros (OFAC), y el Departamento de Impuestos de Nueva York), con la asistencia y apoyo de la oficina del ICE-HIS de Chicago, el Departamento de Justicia de Crímenes Informáticos y Propiedad Intelectual y de Confiscación de Bienes y la Sección de Lavado de Activos, la Oficina del Fiscal del Distrito Sur de Nueva York, y fuerzas del orden público extranjeras, particularmente la Policía Metropolitana e Reykjavik de la República de Islandia, y la Oficina Central de la República de Francia para la Lucha contra el Crimen Relacionado con la Tecnología de la Información y la Comunicación.