

GAFI



DIRECTRICES PARA UN ENFOQUE
BASADO EN RIESGO

MONEDAS VIRTUALES

JUNIO 2015



El Grupo de Acción Financiera Internacional (GAFI) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger el sistema financiero mundial contra el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Las Recomendaciones del GAFI son reconocidas como el estándar global de Antilavado de activos (ALA) y contra la financiación del terrorismo (CFT).

Para obtener más información acerca del GAFI, por favor visite el sitio web:

www.fatf-gafi.org



La presente Directriz se tradujo bajo la responsabilidad del Grupo de Acción Financiera del Caribe (GAFIC).

www.cfatf-gafic.org

© 2015 FATF/OECD. Todos los derechos reservados.

Queda prohibida la reproducción o traducción de esta publicación sin permiso previo y por escrito. Las solicitudes para obtener tal autorización, para la totalidad o parte de esta publicación, deben ser dirigidas a la Secretaría del GAFI, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

TABLA DE CONTENIDO

TABLA DE SIGLAS	2
SECCIÓN I – INTRODUCCIÓN	3
Antecedentes	3
Objetivo de las directrices	4
Alcance de las directrices	5
Estructura	5
SECCIÓN II – ALCANCE DE LOS ESTÁNDARES DEL GAFI	6
Evaluación inicial de riesgo	6
Definiciones del GAFI	6
SECCIÓN III – APLICACIÓN DE LOS ESTÁNDARES DEL GAFI A LOS PAISES Y LAS AUTORIDADES COMPETENTES	8
SECCIÓN IV – APLICACIÓN DE LOS ESTÁNDARES DEL GAFI PARA LAS ENTIDADES CUBIERTAS	12
Posibles soluciones a los desafíos de cumplimiento	14
SECCIÓN V - EJEMPLOS DE PAÍS (O GRUPO DE PAÍSES) DE ENFOQUE BASADO EN RIESGO A VCPDS	16
APÉNDICE A MONEDAS VIRTUALES - DEFINICIONES CLAVE Y LOS RIESGOS POTENCIALES DE ALA/CFT	27
Introducción	27
Definiciones clave:	28
Usos Legítimos	34
riesgos Potenciales	34
Las acciones de las agencias de orden Público involucrando moneda virtual	35
Notas	39
Bibliografía y fuentes	42
APÉNDICE B CÓMO FUNCIONA LA MONEDA VIRTUAL CONVERTIBLE DESCENTRALIZADA COMO UN MECANISMO DE PAGOS	43
Introducción	43
Alcance	43
Participando en la red Bitcoin para enviar y recibir Bitcoins	45

TABLA DE SIGLAS

ALA	Antilavado de Activos
ATM	Cajero Automático
BaFIN	Autoridad Federal alemana de supervisión
DDC	Debida Diligencia del Cliente
CFT	Contra la Financiación del Terrorismo
APNFD	Actividades y Profesiones No Financieras Designadas
EBA	La Autoridad Bancaria Europea
FINMA	Autoridad de Supervisión del Mercado Financiero
KWG	Ley alemana de Banca
MAS	Autoridad Monetaria de Singapur
LA	Lavado de Activos
MSB	Negocios de Servicios Monetarios
STDV	Servicio (s) de Transferencia de Dinero o de Valores
NPPS	Nuevos Productos de Pago y Servicios
P2P	Persona a persona
RBA	Enfoque Basado en Riesgo
FT	Financiamiento Terrorista
MV	Moneda Virtual
VCPPS	Productos y Servicios de Pago de Moneda Virtual

SECCIÓN I – INTRODUCCIÓN

ANTECEDENTES

1. El Grupo de Acción Financiera Internacional (GAFI) emitió el informe [Virtual Currencies Key Definitions and Potential AML/CFT Risks](#), (Monedas Virtuales Definiciones Clave y Riesgos Potenciales de ALA/CFT), en junio de 2014 (Informe de junio de 2014 MV). En los últimos años, las monedas virtuales (MV) han surgido y atraído inversión en infraestructura de pagos basado en los protocolos de software. Estos mecanismos de pagos intentan proporcionar un nuevo método para la transmisión de valor a través del internet.
2. El GAFI reconoce la innovación financiera. Al mismo tiempo, los productos de pago y servicios de MV (VCPSS por sus siglas en inglés) presentan riesgos de lavado de activos y financiamiento terrorista (LA/FT) y otros riesgos de delitos que deben ser identificados y mitigados. Estas Directrices se centran en la aplicación de un enfoque basado en riesgo a los riesgos de LA/FT asociados con VCPSS y no en otros tipos de productos financieros de MV, tales como productos de valores de MV o de futuros. En consecuencia, las Directrices han adoptado el término productos de pagos y servicios de MV (VCPSS), en vez de productos y servicios de MV (VCP), donde la discusión se limita a esquemas de pagos de MV.
3. El desarrollo de VCPSS y las interacciones de los VCPSS con otros Nuevos de Productos y Servicios de Pago (NPPS por sus siglas en inglés) e incluso con servicios de banca tradicional,¹ dan lugar a la necesidad de estas Directrices para proteger la integridad del sistema financiero global.
4. Estas Directrices independientes se basan en el informe de junio de 2014 de MV y en la matriz de riesgo y las mejores prácticas del informe de [Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services](#)² (Directrices para un Enfoque basado en Riesgo a las Tarjetas Prepagados, Pagos Móviles y Servicios de Pago en Internet) (Informe de NPPS de junio de 2013).
5. Estas Directrices forman parte de un enfoque gradual adoptado por el GAFI. El foco de estas Directrices es sobre los puntos de intersección que proporcionan fuentes al sistema financiero regulado, especialmente cambiadores³ de moneda virtual convertible⁴. El GAFI continuará monitoreando los acontecimientos en los VCPSS y los emergentes riesgos y factores atenuantes. Mientras más aprendamos sobre la tecnología y el uso de VCPSS, las Directrices puede ser actualizadas para incluir, en su caso, mejores prácticas que emergen para abordar las cuestiones reglamentarias que surjan en relación con los riesgos de LA/FT asociadas a VCPSS. Cuestiones relacionadas con por ejemplo las transferencias dentro de las redes descentralizadas de MV convertibles que no implican actividades de intercambio, tales como transferencias de persona a persona involucrando “wallet providers” (servidores de proveedores de carteras) y pagos de gran valor de MV, que no están abordados por estas Directrices pueden ser considerados a largo plazo.

OBJETIVO DE LAS DIRECTRICES

6. Estas Directrices pretenden explicar la aplicación del enfoque basado en riesgo a las medidas de ALA/CFT en el contexto de MV; identificar las entidades que participan en VCPSS; y aclarar la aplicación de las *Recomendaciones del GAFI* relevantes para cambiadores de moneda virtual convertible. Estas directrices también pretenden ayudar a las autoridades nacionales a entender y potencialmente desarrollar respuestas reguladoras incluyendo la necesidad de modificar sus leyes nacionales para abordar los riesgos de LA/FT de las VCPSS. Estas Directrices también pretenden ayudar al sector privado a entender mejor las obligaciones de ALA/CFT pertinentes y cómo pueden efectivamente cumplir con los requisitos pertinentes. Las Directrices incorporan el marco conceptual y los términos clave adoptados por el GAFI en el Informe de VC de junio de 2014 (*Apéndice A*) y a los lectores se refieren a ese documento para la discusión de casos de uso potencial para la MV y un glosario de términos.

7. Las Directrices pretenden:

- a) Mostrar como *Recomendaciones del GAFI* específicas deben aplicar a cambiadores de moneda virtual convertible en el contexto de VCPSS, identificar medidas de ALA/CFT que podrían ser requeridas y dar ejemplos; e
- b) Identificar los obstáculos a la aplicación de medidas atenuantes basados en la tecnología de VCPSS y/o modelos de negocio y en marcos legales heredados.

8. El GAFI nota que algunos gobiernos están empezando a considerar una gama de temas regulatorios presentados por VCPSS. Con respecto a ALA/CFT en particular, aunque algunas jurisdicciones están tomando medidas reguladoras, otras están monitoreando y estudiando los acontecimientos y riesgos potenciales de LA/FT, a medida que el uso todavía se desarrolla en aquellas jurisdicciones. Para algunas jurisdicciones, el establecimiento de un régimen regulatorio eficaz de ALA/CFT puede requerir una comprensión más profunda de las VCPSS. Sin embargo, el rápido desarrollo, funcionalidad creciente, creciente adopción y naturaleza global de las VCPSS convierten en prioridad la acción nacional para identificar y mitigar los riesgos de LA/FT presentados por las VCPSS. El GAFI reconoce que pueden existir otras consideraciones de política que puedan afectar las finales opciones o resultados regulatorias de VCPSS en jurisdicciones individuales.

9. Establecer alguna forma de Directrices a lo largo de todas las jurisdicciones que tratan similares productos y servicios constantemente según su función y perfil de riesgo es esencial para mejorar la eficacia de los estándares internacionales de ALA/CFT. Esta es una preocupación particular para las VCPSS dado su carácter 'sin fronteras', donde actividades pueden llevarse a cabo sin parecer ser basadas en cualquier jurisdicción en particular. Mientras que la Directrices no son obligatorias y no anulan el ámbito de las autoridades nacionales, se espera que ayudarán a las autoridades públicas y el sector privado a identificar y efectivamente abordar los asociados riesgos de LA/FT de las VCPSS.

ALCANCE DE LAS DIRECTRICES

10. Las Directrices se centran en las VCPDS y relacionadas cuestiones de ALA/CFT y se aplica tanto a las VCPDS centralizadas como a las descentralizadas. Principalmente aborda la MV convertible, debido a su mayor riesgo. El foco de estas Directrices es en cambiadores de moneda virtual convertibles que son puntos de intersección que proporcionan fuentes al sistema financiero regulado (donde las actividades de MV convertibles cruzan con el sistema financiero regulado de moneda fiat o de uso legal). No se abordan cuestiones no regulatorias de ALA/CFT implicados por mecanismos de pago de la MV (p. ej., protección del consumidor, seguridad prudencial y solidez, impuestos, cuestiones de lucha contra el fraude y estándares de seguridad de la red de TI). Tampoco contempla los usos de no pagar de la MV (p. ej., productos de almacén de valor para propósitos de ahorros o inversión, tales como los derivados, materias primas y los productos de valores) o la dimensión de la política monetaria de las actividades de MV.⁵

ESTRUCTURA

11. Estas Directrices están organizadas como sigue: la Sección II examina la medida en que cambiadores de moneda virtual convertible caen dentro del ámbito de las *Recomendaciones del GAFI*. La Sección III describe la aplicación de las *Recomendaciones del GAFI* a los países y las autoridades competentes; la Sección IV explica la aplicación de las *Recomendaciones del GAFI* a cambiadores de moneda virtual convertible; y la Sección V proporciona ejemplos de país (o grupo de países) con planteamientos regulatorios hasta ahora o esperado en un futuro próximo. El Informe de MV de junio de 2014 está incluido en el **Apéndice A**. Una explicación de lo que es la MV y cómo funciona como un mecanismo de pago, basado en diferentes modelos de negocio y métodos de operación, se encuentra en el **Apéndice B**.

SECCIÓN II – ALCANCE DE LOS ESTÁNDARES DEL GAFI⁶

12. Esta Sección (1) analiza la aplicación del enfoque basado en riesgo de las VCPDS y (2) examina cómo los cambiadores de moneda virtual convertible deben ser sujetos a requisitos de ALA/CFT cubiertos por los estándares internacionales.

EVALUACIÓN INICIAL DE RIESGO⁷

13. La evaluación de riesgo en el Informe de MV de junio de 2014 (Apéndice A) indica que al menos a corto plazo, solamente MV *convertible*, que puede utilizarse para mover valor dentro y fuera de las monedas fíat y el sistema financiero regulado, es probable que presente riesgos de LA/FT. Por consiguiente, bajo el enfoque RBA, los países deben centrar sus esfuerzos de ALA/CFT en las MV convertibles de alto riesgo.

14. La evaluación de riesgo también sugiere que los controles de ALA/CFT deben dirigirse a los nodos o eslabones dentro de una estructura de MV convertible—es decir, puntos de intersección que proporcionan fuentes al sistema financiero regulado - y no pretender regular a los usuarios que obtengan MV para la compra de bienes o servicios. Estos nodos incluyen a los cambiadores terceros de MV convertible. Donde ese es el caso, deben ser regulados bajo *las Recomendaciones GAFI*. Así, los países deberían considerar la aplicación de los correspondientes requisitos de ALA/CFT especificados por los estándares internacionales a los cambiadores de MV convertible, y cualquier otro tipo de institución que actúa como nodos donde actividades de MV convertible cruzan con el sistema financiero regulado de moneda fíat.

15. Bajo el RBA, los países también podrían considerar la regulación de instituciones financieras o APNFD que envían, reciben y almacenan MV, pero no ofrecen servicios de cambio o de cobrar/pagar de efectivo entre moneda virtual y fíat. Esto sin embargo, no está en el ámbito de estas Directrices.

DEFINICIONES DEL GAFI

16. *Las Recomendaciones del GAFI* requieren que todas las jurisdicciones impongan requisitos de ALA/CFT especificados a las instituciones financieras y actividades y profesiones no financieras designadas (APNFD) y para asegurar el cumplimiento de esas obligaciones.

17. El GAFI define a una "institución financiera" como cualquier persona natural o jurídica que lleve a cabo como negocio una o más de varias actividades específicas para o en nombre de un cliente. Las categorías potencialmente más relevantes a las VCPDS actualmente disponibles incluyen las personas que llevan a cabo como un negocio: Servicio (s) de transferencia de dinero o valor (STDV)⁸; aceptación de depósitos y otros fondos reembolsables del público; emisión y gestión de medios de pago; y el comercio en moneda extranjera o valores negociables. Dependiendo de sus actividades particulares, cambiadores de MV descentralizados, wallet providers (proveedores de cartera) y procesadores/remitentes de pagos, así como otros posibles modelos de negocio de MV, pueden caer dentro de uno o más de estas categorías.

18. Si una persona natural o jurídica dedicada a VCPDS es una entidad obligada depende de cómo esa persona utiliza la MV y en beneficio de quién. Las autoridades nacionales deben abordar los riesgos de LA/FT asociados con actividades de cambio de MV convertible (cuando actividades de MV convertibles cruzan con el sistema financiero regulado de moneda fíat), según corresponda bajo sus marcos jurídicos nacionales, que pueden ofrecer una variedad de opciones para la regulación de dicha actividad.
19. Proveedores de VCPDS que realizan actividades que caen dentro de la definición de GAFI de *una institución financiera* están sujetos a las aplicables Recomendaciones del GAFI. Esto incluye a cambiadores de moneda virtual convertible cuando las actividades de MV convertible cruza con el sistema financiero regulado de moneda fíat.
20. Dependiendo de la intensidad o volumen de las actividades específicas de MV involucradas y sus propios marcos jurídicos nacionales, los países deben abordar los riesgos de LA/FT asociados con cambios de MV y cualesquier otros tipos de instituciones que actúan como nodos cuando las actividades de MV convertible cruzan con el sistema financiero regulado de moneda fíat, mediante la aplicación de las Recomendaciones del GAFI pertinentes a cualquiera de estas categorías de entidades cubiertas , sobre una base de riesgo.

SECCIÓN III – APLICACIÓN DE LOS ESTÁNDARES DEL GAFI A LOS PAISES Y LAS AUTORIDADES COMPETENTES

21. Esta Sección explica cómo Recomendaciones del GAFI específicas relacionadas con VCPSS se aplican a los países y las autoridades competentes, centrándose en la identificación y mitigación de riesgos asociados a MV convertible, aplicando los requisitos de licencias/registro, implementación de supervisión efectiva, proporcionando una gama de sanciones efectivas y disuasorias y facilitando la cooperación nacional e internacional.

22. Algunas de las Recomendaciones del GAFI son directamente relevantes para la comprensión de cómo los países deben utilizar a las autoridades del gobierno y la cooperación internacional para abordar los riesgos de LA/FT con MV convertible.

23. **Recomendación 1.** Las actuales *Recomendaciones de GAFI* dejan claro que los países deben aplicar un RBA para asegurar que las medidas para prevenir o mitigar los riesgos de LA/FT son acordes con los riesgos identificados. Bajo la RBA, los países deben fortalecer los requisitos para situaciones de riesgos más altos. Al evaluar el riesgo de LA/FT de MV convertible, la distinción entre MV centralizada y descentralizada será un aspecto clave. Debido al anonimato y los retos para llevar a cabo una correcta identificación del participante, los VCPSS convertibles descentralizados en general pueden ser considerados de mayor riesgo de LA/FT que requerirá la aplicación de medidas mejoradas de debida diligencia.

24. La Recomendación 1 requiere que los países identifiquen, comprendan y evalúen los riesgos de LA/FT del país y que tomen medidas orientadas a mitigar eficazmente los riesgos. Este requisito se aplica en relación con los riesgos asociados con las MVs y otras nuevas tecnologías. La Cooperación entre el sector público y privado puede ayudar a las autoridades competentes en el desarrollo de las políticas ALA/CFT para las actividades financieras de MV, las innovaciones en servicios y productos emergentes y tecnologías de MV. Esto puede también ayudar a los países en la asignación y priorización de recursos de ALA/CFT por autoridades competentes.

25. Las autoridades nacionales deberían considerar realizar una evaluación de riesgos coordinada de productos y servicios de MV que (1) permita a todas las autoridades pertinentes entender cómo determinados productos y servicios de MV funcionan, encajan e impactan a todas las jurisdicciones reguladoras pertinentes para fines de ALA/CFT (p. ej., mecanismos de transmisión y pagos de dinero; Cajeros automáticos de MV; productos básicos; valores) y (2) promueva similar tratamiento de ALA/CFT para productos y servicios similares con similares perfiles de riesgo.

26. Los países también deberán requerir a las instituciones financieras y las APNFD identificar, evaluar y tomar medidas efectivas para mitigar sus riesgos de LA/FT asociados con las VCPSS. Para los propósitos de ALA/CFT, donde se permiten actividades VCPSS bajo derecho nacional, las jurisdicciones, instituciones financieras y APNFD, incluso los cambiadores de moneda virtual convertible, deben evaluar los riesgos de LA/FT y aplicar un RBA para asegurar que se implementen las medidas adecuadas para prevenir o mitigar esos riesgos.

27. Incluso si un país decide no regular MV con respecto a los riesgos no de LA/FT, tales como protección del consumidor, seguridad prudencial y solidez y seguridad de la red, todavía debe tomar rápida acción para identificar, evaluar y aplicar un RBA para mitigar los riesgos de LA/FT asociados con MV bajo las pertinentes Recomendaciones del GAFI.

28. Según esta evaluación de riesgo, los países deberían decidir regular plataformas de intercambios entre las monedas virtuales convertibles y monedas fiat (es decir, cambiadores de moneda virtual convertible). Algunos países podrán decidir prohibir actividades de MV, basadas en su propia evaluación de riesgo (incluyendo, por ejemplo, las tendencias de entrada al mercado) y el contexto regulatorio nacional para apoyar otros objetivos de política no abordados por estas Directrices (p. ej., protección del consumidor, seguridad y solidez, política monetaria). Donde los países consideran prohibir VCPSS, deberían tener en cuenta, entre otras cosas, el impacto que tendría una prohibición en el nivel local y global de los riesgos de LA/FT, incluyendo si el prohibir las actividades de pago de MV podría conducirlos a pasar a la clandestinidad, donde seguirán operando sin controles de ALA/CFT o supervisión. Independientemente de si un país opta por prohibir o regular las MV, medidas adicionales son útiles para mitigar el riesgo general de LA/FT. Si un país decide prohibir actividades de MV, las medidas de mitigación adicionales incluirían identificar proveedores de MV que operan ilegalmente en su jurisdicción y la aplicación de sanciones disuasivas y proporcionadas a ellos. La prohibición aún requeriría acercamiento, educación y acciones de ejecución por el país. Los países también tendrían que tener en cuenta el elemento transfronterizo de las VCPSS en sus estrategias de mitigación de riesgo.

29. **Recomendación 2** requiere cooperación y coordinación nacional con respecto a las políticas de ALA/CFT--incluso en el sector de MV. Los países pueden considerar establecer mecanismos, tales como grupos de trabajo interinstitucionales, para permitir a los responsables de políticas, reguladores, supervisores, la unidad de inteligencia financiera (UIF) y autoridades de orden público cooperar uno con el otro y cualquier otras autoridades competentes pertinentes para desarrollar e implementar políticas, reglamentos y otras medidas eficaces para abordar los riesgos de LA/FT de MV.

30. Los países pueden considerar el desarrollo de mecanismos de coordinación nacional que facilitan la regulación apropiada de ALA/CFT basada en riesgo y supervisión a través de diversos productos y servicios de MV. Entre otras cosas, las autoridades nacionales pueden realizar una evaluación de riesgo de VCPSS que (1) permita a todas las autoridades pertinentes entender cómo determinados productos y servicios de MV funcionan, encajan e impactan a todas las jurisdicciones reguladoras para fines de ALA/CFT (p. ej., sistemas de transmisión y pagos de dinero; Cajeros automáticos MV; productos básicos; valores) y (2) promueva similar tratamiento de ALA/CFT para productos y servicios similares con similares perfiles de riesgo. Los países también deberían considerar la adopción de su (s) mecanismo (s) de cooperación y coordinación nacional que facilite la participación con el sector privado de MV.

31. Si la MV se desarrolla en una parte significativa del sector financiero, los países deberían considerar examinar la relación entre la regulación y supervisión de ALA/CFT de MV y la regulación y supervisión de ALA/CFT de las MV (p. ej., protección del consumidor, seguridad y solidez, seguros, seguridad de red, cumplimiento tributario). En este sentido, se recomienda que los

países deberían considerar emprender trabajo de corto y largo plazo de política para desarrollar regulación integral de la VCPSS si se produce la adopción generalizada de MV.

32. **Recomendación 14** demanda a los países registrar u otorgar licencias a personas naturales o jurídicas que proporcionan STDV en el país y asegurar el cumplimiento de las medidas de ALA/CFT pertinentes. Esto incluye someter a los STDV que operan en el país al monitoreo para el cumplimiento de las medidas de inscripción/otorgación de licencias y otras medidas de ALA/CFT aplicables.

33. Los requisitos de registro/otorgación de licencia de la Recomendación 14 se aplican a las entidades nacionales que ofrecen servicios de cambio de MV convertible entre MV y moneda fiat (es decir, VCPSS) en una jurisdicción.

34. Porque los cambiadores de MV convertible que transfieren valor digitalmente, a través del internet, no están sujetos a límites territoriales y generalmente ofrecen VCPSS a las personas en países en los que no están físicamente presentes, es muy importante que todos los países de origen apliquen requisitos internos otorgación de licencia o registro cuando sea requerido por las Recomendaciones del GAFI. Por las mismas razones, la adecuada supervisión por la jurisdicción local y la adecuada cooperación e intercambio de información entre autoridades competentes entre jurisdicciones donde la entidad presta servicios es de alta importancia.

35. **Recomendación 15** refuerza la obligación fundamental de RBA con respecto a las nuevas tecnologías. Requiere que los países identifiquen y evalúen los riesgos de LA/FT relacionadas con el desarrollo de nuevos productos y nuevas prácticas de negocio, incluso nuevos mecanismos de entrega y el uso de tecnologías nuevas o en desarrollo para tantos productos nuevos y existentes. La Recomendación 15 también requiere que los países aseguren que las instituciones financieras licenciados por u operando en su jurisdicción adopten medidas apropiadas para manejar y mitigar el riesgo *antes* del lanzamiento de nuevos productos o prácticas comerciales o la utilización de tecnologías nuevas o en desarrollo. Los requisitos nacionales con respecto a las nuevas tecnologías deben incluir a los VCPSS.

36. **Recomendación 16** establece los requisitos para los países con respecto a transferencias electrónicas. La Recomendación 16 se aplica a transferencias electrónicas transfronterizas y transferencias electrónicas nacionales. Una transferencia electrónica se refiere a cualquier transacción realizada en nombre de un originador (a) a través de una institución financiera (b) por medios electrónicos con el fin de disponer de una cantidad de fondos a una persona beneficiaria o (c) en una institución financiera beneficiaria, independientemente de si el ordenante y el beneficiario son la misma persona. Los países deben asegurar que cuando cambiadores de moneda virtual convertible llevan a cabo transferencias de MV convertible que son transferencias electrónicas, que incluyen la información requerida sobre el ordenante y el beneficiario especificada por Recomendación 16. En este sentido, los países pueden adoptar un umbral *de minimis* para transferencias electrónicas transfronterizas no superiores a 1 000 USD/EUROS. También los países deben asegurar que las instituciones financieras monitoreen las transferencias de MV convertible para detectar aquellos que carecen de la información requerida sobre el originador y/o beneficiario y tomen las medidas apropiadas para abordar esa situación si se produce.

37. **Recomendación 26** requiere que los países aseguren que los cambiadores de MV convertible que actúan como nodos cuando las actividades de MV cruzan con el sistema financiero regulado de moneda fíat están sujetas a una reglamentación y supervisión adecuada. Los países deberían considerar la modificación de marcos legales heredados, según sea necesario, para autorizar la regulación eficaz de ALA/CFT de los mecanismos de pago de MV descentralizados.

38. **Recomendación 35** dirige a los países a tener una gama de sanciones efectivas, proporcionadas y disuasivas (penales, civiles o administrativas) disponible para tratar a personas naturales o jurídicas cubiertas por Recomendaciones 6 y 8 a 23, que faltan en cumplir con los requisitos de ALA/CFT aplicables. Sin embargo, en la actualidad, VCPSS, sobre todo los VCPSS convertible descentralizados, presentan numerosos desafíos para la aplicación de herramientas de orden público tradicionales y llevar a cabo enjuiciamientos exitosos. El anonimato actual de la mayoría de transacciones MV descentralizadas se le hace difícil determinar la identidad de las personas involucradas. Los protocolos subyacentes sobre los cuales actualmente se basan casi todos los VCPSS descentralizadas no requieren ni proporcionan identificación y verificación de los participantes. Por otra parte, los registros históricos de las transacciones generados en el blockchain (cadena de bloque) por los protocolos subyacentes no están necesariamente asociados con la identidad del mundo real. Este nivel de anonimato limita la utilidad de la blockchain para el monitoreo de transacciones e identificar actividades sospechosas y presenta un desafío significativo a la capacidad de las agencias de orden público rastrear activos ilícitos que son lavados utilizando MV convertible descentralizada. Además las agencias de orden público no pueden dirigirse a una ubicación central o entidad para fines investigativos. Estos desafíos socavan la capacidad de emplear las sanciones efectivas y disuasivas. Países deben llevar a cabo una revisión de los desafíos que existen en su contexto de país para identificar posibles brechas y tomar medidas, según proceda. La otorgación de licencia o registro de cambiadores de MV y la aplicación de requisitos de identificación/verificación y mantenimiento de registros del cliente, podrían proporcionar una vía que permite que los países aplicar mejor sanciones efectivas y disuasorias en el contexto de MV.

39. **Recomendación 40** exige que los países proporcionen cooperación internacional eficiente y eficaz para ayudar a otros países a combatir LA, delitos determinantes asociados y FT — incluyendo la asistencia legal mutua (**Recomendación 37**); ayudar a identificar, congelar, decomisar y confiscar activos y los instrumentos del delito que pueden adoptar la forma de MV (**Recomendación 38**); y asistencia de extradición efectiva en el contexto de delitos relacionados con moneda virtual (**Recomendación 39**). Estos requisitos también pueden aplicarse a la cooperación que implica la MV. También es importante que las UIF deben cooperar e intercambiar información sobre los RTS con sus pares, especialmente en relación con operaciones de MV transfronterizas. Suficiente supervisión y control regulatorio de VCPSS convertible operando en su jurisdicción permite a los países a brindar mejor asistencia investigatoria y otra cooperación internacional en el espacio de MV. En la actualidad, la falta de capacidad de regulación e investigación de MV en la mayoría de los países puede presentar obstáculos a la capacidad de los países para proporcionar cooperación internacional significativa. Por otra parte, muchos países no cuentan con marcos legales que les permiten tipificar ciertas actividades de LA/FT de MV, que puede impedirles prestar ALM efectiva en situaciones donde se requiera la doble incriminación (dualidad criminal).

SECCIÓN IV – APLICACIÓN DE LOS ESTÁNDARES DEL GAFI PARA LAS ENTIDADES CUBIERTAS

40. Esta Sección explica cómo *Recomendaciones del GAFI* específicas deben aplicarse a cambios de MV Convertible y cualquier otro tipo de entidades que actúan como nodos cuando las actividades de MV convertible cruzan con el sistema financiero regulado de moneda fiat, para mitigar los riesgos de LA/FT asociados con los VCPSS. Estas deberían incluir aplicar un RBA (Recomendación 1), a debida diligencia del cliente (DDC) (Recomendación 10); mantenimiento de registros (Recomendación 11); requisitos de registro u otorgación de licencias para los STDV (Recomendación 14) identificación y mitigación de los riesgos asociados con las nuevas tecnologías (Recomendación 15); Requisitos del programa de ALA/CFT (Recomendación 18) y reporte de transacciones sospechosas (Recomendación 20). Esta sección también examina los obstáculos actuales a la aplicación de algunas de estas medidas de mitigación en el espacio de MV descentralizada. Recomendación 14 se discute solamente en la Sección III arriba, pero como se nota requiere que las entidades cubiertas cumplan con los requisitos de registro u otorgación de licencia en todas jurisdicción donde prestan STDV de MV.

41. **Recomendación 1.** Las *Recomendaciones de GAFI* dejan claro que los países deberían exigir a las instituciones financieras y las APNFD identificar, evaluar y tomar medidas efectivas para mitigar sus riesgos de LA/FT (incluyendo aquellos asociados con VCPSS). Esto incluye esfuerzos en curso para perfeccionar los procesos técnicos utilizados para fiablemente identificar y verificar a los clientes. Para propósitos de ALA/CFT, donde se permiten actividades de MV bajo derecho nacional, todas jurisdicciones, instituciones financieras y APNFD, incluso cambiadores de moneda virtual convertible, deben evaluar los riesgos de LA/FT que plantea actividades de MV y aplicar un RBA para asegurar que se apliquen las medidas adecuadas para prevenir o mitigar esos riesgos. El RBA no implica la negación automática o total de servicios a VCPSS sin una evaluación adecuada de riesgos.

42. **Recomendación 10.** La Debida Diligencia del Cliente (DDC) es una medida esencial para mitigar los riesgos de LA/FT asociados con MV convertible. Conforme a los Estándares del GAFI, los países deben exigirle a los cambiadores de MV convertible realizar debida diligencia del cliente al establecer relaciones comerciales o al realizar transacciones ocasionales (no electrónicas) utilizando documentos fuentes fiables e independientes, datos o información.⁹ Por ejemplo, cambiadores de MV convertible deben ser exigidos a realizar debida diligencia del cliente al cambiar MV para moneda fiat o viceversa en una transacción única mayor que el umbral designado de USD/EUROS, 15 000 o (b) llevar a cabo transacciones ocasionales que son transferencias electrónicas cubiertas por la Recomendación 16 y su Nota Interpretativa. Generalmente, las transacciones de MV convertible implicarán a una transferencia electrónica y por lo tanto, estar sujeto a la Recomendación 16.

43. Países pueden desear considerar tener un umbral más bajo o ninguno para los requisitos de DDC de MV en su caso, dada la naturaleza y el nivel de riesgos de LA/FT identificado.

44. A la luz de la naturaleza de la VCPSS, en las cuales se establecen las relaciones de cliente, fondos cargados y transacciones transmitidas completamente a través del internet, las instituciones necesariamente deben recurrir a la verificación e identificación no cara a cara. Los países deberían

considerar requerir que las entidades que ofrecen VCPSS sigan las mejores prácticas sugeridas en las *Directrices de NPPS de junio de 2013*. Estas, en la medida aplicable, incluyen: corroborar la información de identidad recibida del cliente, tales como el número de identidad nacional, con información en bases de datos de terceros o de otras fuentes confiables; potencialmente rastreando la dirección de Protocolo Internet (IP) del cliente; y buscando en la Web para corroborar información de actividad coherente con el perfil de transacciones del cliente, siempre que la recopilación de datos esté en consonancia con la legislación nacional de privacidad.

45. En casos donde VCPSS convertibles presentan mayor riesgo, según lo determinado sobre la base de la RBA, se debe exigir a los cambiadores de moneda virtual convertible el llevar a cabo DDC mejorada o intensificada en proporción a ese riesgo y ser animados a utilizar varias técnicas para tomar medidas razonables para verificar la identidad del cliente. En casos donde se permita a los cambiadores de moneda virtual convertible completar la verificación después de establecer la relación comercial con el fin de no interrumpir la realización normal de negocios (en casos de bajo riesgo), deben exigirse el completar la verificación antes de llevar a cabo transacciones ocasionales por encima del umbral.

46. Los países deben esperar también que las instituciones financieras y las APNFD consideren los riesgos asociados con la fuente de financiación de VCPSS convertible. VCPSS convertibles descentralizadas permiten anónimas fuentes de financiación, incluyendo transferencias persona a persona (P2P) de MV y financiación por las NPPS que también son anónimos, aumentando los riesgos de LA/FT. Como con las NPPS, los negocios de VCPSS debe considerar, para las transacciones ocasionales por encima de un determinado umbral, limitar la fuente de fondos a una cuenta bancaria, tarjeta de débito o crédito, o al menos aplicar tales limitaciones a la carga inicial, o un período determinado hasta que se puede establecer un patrón de transacción o para carga por encima de un umbral determinado.

47. El monitoreo de transacciones es un mitigante clave de riesgo en el espacio de MV convertible debido a la dificultad de verificación de identidad no cara a cara y porque es sólo recientemente que la tecnología de MV convertible descentralizada permite ciertas mitigantes de riesgo que pueden estar disponibles para las NPPS ser incluidas en VCPSS descentralizadas con el fin de restringir la funcionalidad y reducir el riesgo. Por ejemplo, la tecnología de firmas múltiples (multi-sig) ahora permite a los VCPSS incluir con eficacia cargar el valor total de la cartera y límites de valor/velocidad de transacción en VCPSS descentralizadas. Sin embargo, tecnología MV descentralizada actual no hace posible incluir eficazmente los límites geográficos; limitar el uso para la compra de ciertos bienes y servicios; o impedir a las transferencias de persona a persona.

48. Se recomienda que los países insten al monitoreo de transacciones, acorde con el riesgo. La naturaleza pública de la información de transacción disponible en el blockchain teóricamente facilita el monitoreo de transacciones, pero como se notó en *el Informe de MV de junio de 2014* (Apéndice A), la falta de identidad del mundo real asociados con muchas transacciones de MV descentralizadas limita la utilidad del blockchain para monitorear las transacciones e identificar actividades sospechosas, que presenta serios desafíos al cumplimiento eficaz de ALA/CFT y la supervisión.

49. **Recomendación 11, recomendación 20 y recomendación 22. Mantenimiento de registros y el Reporte de actividades sospechosas** cuando las transacciones de MV podrían

involucrar los activos de actividad criminal o estar relacionado con el financiamiento del terrorismo, de acuerdo con la Recomendación 20, son también esenciales. Como mínimo, a las instituciones financieras y las APNFD debe exigírseles el mantener registros de transacciones que incluyan: información para identificar a las partes; las claves públicas, direcciones o cuentas involucradas; la naturaleza y la fecha de la transacción y el importe transferido. La información pública disponible en la blockchain proporciona una base de principio para el mantenimiento de registros, siempre y cuando las instituciones pueden identificar adecuadamente a sus clientes. Los países deben exigir a las instituciones estar atentos al tipo de actividad sospechosa que ellas se encuentran en una posición para detectar.

50. **Recomendación 15 y Recomendación 22** específicamente abordan las nuevas tecnologías y requiere que las instituciones financieras y las APNFD identifiquen y evalúen los riesgos de LA/FT relacionadas con el desarrollo de nuevos productos y nuevas prácticas de negocio, incluso nuevos mecanismos de entrega o distribución y el uso de tecnologías nuevas o en desarrollo de productos nuevos y existentes. Recomendación 15 también requiere que las instituciones financieras y las APNFD autorizado por u operando en una jurisdicción a que tomen medidas apropiadas para manejar y mitigar el riesgo *antes* del lanzamiento de nuevos productos o prácticas comerciales o la utilización de tecnologías nuevas o en desarrollo. Estas medidas aplican en relación con la MV como una nueva tecnología. Se espera que las autoridades nacionales ejecutaran esta obligación y que las instituciones financieras y las APNFD deben ser proactivas en el cumplimiento de las expectativas establecidas en la Recomendación 15.

POSIBLES SOLUCIONES A LOS DESAFÍOS DE CUMPLIMIENTO

51. Las instituciones financieras y las APNFD deben ser obligados a cumplir con los requisitos de identificación y verificación del cliente y de monitoreo de transacciones para VCPDS convertible descentralizadas, utilizando los medios más eficaces y eficientes disponibles, en cuanto tales productos y servicios se ofrezcan. Teniendo en cuenta los desafíos de cumplimiento y de orden público presentados por la MV convertible descentralizada, las instituciones financieras, APNFD, desarrolladores, inversores y otros actores en el espacio de MV deberían buscar desarrollar soluciones basadas en tecnología que mejorarán el cumplimiento.

52. Por ejemplo, los desarrolladores pueden ser capaces de crear nuevas tecnologías de MV, tales como interfaces de programación de aplicaciones (API por sus siglas en inglés) que proporcionan información de identificación del cliente, o permiten a las instituciones financieras o las APNFD limitar el tamaño y velocidad de la transacción o establecer una variedad de condiciones que deben cumplirse antes de que una transacción de MV puede enviarse al destinatario/beneficiario para reducir los riesgos de LA/FT asociados con una particular VCPDS. La posibilidad de utilizar información recopilada en línea para aumentar el perfil del cliente y ayudar en la detección de transacciones y actividades sospechosas es otra área de crecimiento importante de cumplimiento ALA/CFT. Innovación relevante al cumplimiento ALA/CFT puede tomar la forma de mejorar los protocolos existentes de MV o desarrollar MVs completamente nuevas, construidos en los protocolos subyacentes fundamentalmente diferentes que pueden incluir mitigantes de riesgo o facilitar la identificación del cliente y el monitoreo de transacciones.

53. Los sistemas de identidad digital de terceros también pueden ser desarrollados para facilitar el cumplimiento de ALA/CFT que podría mejor ajustarse a VCPSS. Estos sistemas podrían, por ejemplo, involucrar a los custodios de identidad digital de terceros y/u otras entidades creando, autenticando y manteniendo soluciones de identidad digital para fines específicos de DDC, monitoreo, y a efectos de reporte, en respuesta a los requisitos impuestos por las leyes nacionales de ALA/CFT implementando los estándares internacionales. En cuanto a los custodios de identidad digital de terceros, ellos mismos tendrían que ser regulados para asegurar la integridad de la identificación/verificación.

54. Las instituciones financieras y las APNFD también podrían explorar modelos de negocio en desarrollo para facilitar la identificación/verificación de clientes, monitoreo de transacciones y cumplimiento de otros requisitos de ALA/CFT relevantes. Por ejemplo, instituciones involucradas en la transmisión de MV convertible descentralizada podrían considerar crear una (s) asociación (es) de industria integrada por instituciones de MV investigadas y desarrollar políticas y prácticas para los miembros que les permiten identificar transacciones específicas como procedente de un miembro que ha aplicado DDC apropiado y está llevando a cabo monitoreo apropiado de transacciones.

SECCIÓN V - EJEMPLOS DE PAÍS (O GRUPO DE PAÍSES) DE ENFOQUE BASADO EN RIESGO A VCPPTS

55. Esta Sección da un resumen de los enfoques regulatorios que algunos países (o grupo de países) han adoptado hasta la fecha, así como los enfoques esperados por países en el futuro cercano. Como se mencionó en la Introducción, los gobiernos de todo el mundo están comenzando a lidiar con la amplia gama de desafíos regulatorios presentados por VCPPTS. Un informe por el Banco de Pagos Internacionales clasifica las medidas tomadas hasta la fecha como sigue.¹⁰

- a) Imponer restricciones a las entidades reguladas para hacer frente a las monedas virtuales;
- b) Adoptar medidas legislativas/regulatorias, tales como la necesidad plataformas de cambio que tratan con MV ser objeto de regulación como los remitentes de dinero, o la propuesta regulación de los intermediarios de MV en algunas jurisdicciones para fines de ALA/CFT;
- c) Publicar declaraciones advirtiendo a los usuarios sobre los riesgos asociados con la MV y/o clarificar la posición de las autoridades con respecto a la MV; y
- d) Monitorear y estudiar los acontecimientos.

56. Los actuales o previstos enfoques regulatorios de ALA/CFT a MV adoptado en un número de jurisdicciones que se detallan a continuación ofrecen ejemplos de la RBA:

CANADÁ

57. En junio de 2014, Canadá modificó su legislación de ALA/CFT para tratar a las personas y entidades que participan en el negocio de lidiar con MV como una Empresas de Servicios Monetarios (MSB por sus siglas en inglés). Las regulaciones de respaldo están todavía bajo desarrollo para definir exactamente cuales entidades serán cubiertas y sus respectivas obligaciones. Sin embargo, se espera que las obligaciones serán en gran parte similares a las existentes obligaciones de las MSB, que incluyen inscripción, DDC (incluyendo información de beneficiario final), mantenimiento de registro y un régimen de cumplimiento interno, así como el reporte de transacciones sospechosas y ciertas prescritas.

58. En el desarrollo de su política de ALA/CFT de MV, Canadá está tomando un RBA, incluyendo entender los riesgos asociados con la MV en el contexto de los riesgos de LA/FT que enfrentan Canadá, como parte de Evaluación Nacional de Riesgo LA/FT de Canadá. Las regulaciones darán balance a las necesidades de mitigar el riesgo de LA/FT con los de fomentar innovación financiera continua. Por lo tanto, Canadá propone una intervención reguladora dirigida en las áreas con las mayores vulnerabilidades de LA/FT.

CHINA

59. El 3 de diciembre de 2013, el Banco de China Popular, conjuntamente con el MIIT (Ministerio de Industria y Tecnología de la Información), la Comisión Reguladora Bancaria (CBRC), la Comisión Reguladora de Seguros (CIRC) y la Comisión Reguladora de Valores (CSRC) emitió el *Aviso sobre la*

Prevención de Riesgos de Bitcoin. Este aviso requería que las instituciones que ofrecen servicios, incluyendo el registro de bitcoin, carpeta de bitcoin e cambio de bitcoin deberán cumplir con las obligaciones de ALA/CFT y tomar medidas para identificar a sus clientes y registrar la información de identificación. Instituciones financieras y proveedores de servicios de pago también fueron obligados a tomar medidas de supervisión mejoradas con respecto a los proveedores de servicios de bitcoin para prevenir los riesgos relevantes. Además, las sucursales PBC en el país debían estudiar a riesgos de LA relacionados con bitcoin y tomar acciones proporcionales incluyendo acciones de mejorada supervisión y monitoreo de transacciones sospechosas para mitigar los riesgos.

LA OPINIÓN DE EBA SOBRE "MONEDAS VIRTUALES"

60. El 04 de julio de 2014, la Autoridad Bancaria Europea (EBA por sus siglas en inglés) emitió una Opinión sobre "monedas virtuales", tras un análisis de los riesgos que estos nuevos productos podrían presentar como mucho ya que no están regulados. La opinión de la EBA está dirigida a legisladores de UE, así como las autoridades nacionales de supervisión en los 28 Estados Miembros.

61. La Opinión de la EBA está construida alrededor de las recomendaciones a largo y corto plazo con el objetivo de establecer un enfoque regulatorio integral.

62. Desde la perspectiva de la EBA, un potencial enfoque regulatorio a largo plazo requeriría un cuerpo substancial de regulación y tendría que comprender, entre otros elementos, los requerimientos de gobernanza para varios participantes del mercado, la segregación de cuentas de clientes, requisitos de capital y la creación de un "autoridades de gobierno de esquema" que son responsables de la integridad de un sistema de moneda virtual y sus componentes claves, incluyendo su borde protocolo y de transacción.

63. Sin embargo, mientras que no existe ese tipo de régimen, la opinión de EBA considera que algunos de los riesgos más acuciantes identificados deberán ser mitigados por otros medios. Como una "respuesta inmediata", la EBA informa a las autoridades nacionales a sensibilizar a las instituciones financieras de los riesgos de, y disuadirlos de la compra, tenencia o venta de monedas virtuales. La EBA recomienda también que los legisladores de la UE consideren declarar cambios de moneda virtual como 'entidades obligadas' que deben cumplir con los requisitos de antilavado de activos y el financiamiento del terrorismo establecidos en la Directiva Europea Antilavado de Activos. Las negociaciones de la Comisión sobre la IV Directiva sobre antilavado de activos no adoptó la recomendación de julio de 2014 de la EBA. En cambio, la Comisión evaluará opciones para regulación más completa en el mediano plazo. Su próxima evaluación de riesgo ALA/CFT supranacional incluirá una evaluación de los riesgos planteados por MV y hará las recomendaciones pertinentes a los Estados Miembros.

FRANCIA

64. El 29 de enero de 2014, el French Prudential Supervisory and resolution Authority (la Autoridad Prudencial Francesa de Supervisión y Resolución) (ACPR) emitió una declaración de postura, haciendo hincapié en que una entidad dedicada a la intermediación con respecto a la compra o venta de MV a cambio de la moneda fiat es un intermediario financiero que recibe fondos

en nombre de un tercero, y que estas actividades deben ser autorizadas por el ACPR y por lo tanto están sujetas a requisitos de ALA/CFT. En junio de 2014, la UIF francesa, TRACFIN, publicó un informe, "La Regulación de Monedas Virtuales: Recomendaciones para evitar que las monedas virtuales se utilicen para fines fraudulentos y el lavado de activos" prevista para establecer un marco para disuadir el uso de monedas virtuales para fraude y el lavado de activos.

ALEMANIA

65. La Autoridad alemana Federal de Supervisión (BaFin) califica a Bitcoin con efecto legalmente obligatorio como instrumentos financieros en la forma de unidades de cuenta de conformidad con la Sección 1 (11) sentencia 1 de la Ley de Banca Alemana (KWG). Estas unidades son comparables a las monedas, pero no están denominadas como moneda de curso legal.

66. Bitcoin no es dinero electrónico en el sentido del significado de la Ley de Supervisión de Servicios de Pago de Alemania (ZAG), porque en ningún Bitcoin se emite lo que representa un crédito de un emisor. Esto es diferente para las monedas virtuales, que son respaldadas por un emisor central. Bitcoin tampoco es considerado moneda de curso legal, y por lo tanto no califica ni como monedas ni como billetes y monedas.

67. Las actividades comerciales relacionadas con instrumentos financieros generalmente requieren una licencia de BaFin. Pero BaFin también ha aclarado que el uso de Bitcoin como sustituto de moneda para el pago de comercio en sí no es una actividad sujeta a autorización bajo el KWG. La minería de Bitcoin por sí no es una actividad también sujeta a autorización, porque los mineros no emiten ni colocan cualquier Bitcoin ellos mismos. Lo mismo se aplica a la compra o venta de Bitcoin minada o adquirido, que no requiere de autorización tampoco.

68. Sin embargo, un requisito de autorización puede surgir si hay factores adicionales. Bitcoin se cotiza a menudo a través de las plataformas de internet, algunos de los cuales se conocen como intercambios. Generalmente esas actividades requieren autorización de la BaFin. Cuál autorización se requiere sólo puede determinarse mediante el análisis de la implementación técnica y contractual de las transacciones en detalle. Algunos pueden llevar a cabo corretaje de inversión tal como se define en el KWG, otros pueden operar un centro de comercio multilateral, que es un servicio financiero especificado en el KWG. Hay algunos que podrían considerarse como servicios de corretaje principales. Si los compradores y vendedores potenciales simplemente se introducen mutuamente en plataformas, esto no constituye la intermediación de transacciones específicas. En tales casos, sin embargo, los proveedores de estos tipos de plataformas son comerciantes propietarios sujetos a un requisito de autorización en el sentido del KWG. Los proveedores que actúan como casas de cambio que ofrecen cambiar monedas legales directamente a Bitcoin también cumplen con el criterio de comercio propietario sujetos a un requisito de autorización.

69. Puesto que cada caso es diferente, los grupos de minería, es decir, la puesta en común de equipo de potencia de procesamiento en general por varias personas para los fines de generar conjuntamente Bitcoin, no son necesariamente sujetos a supervisión. Como regla general, si varias personas utilizan la potencia de procesamiento con igualdad de derechos y posteriormente distribuyen la Bitcoin proporcionalmente, esto no es una actividad que requiera autorización. Diferentes reglas pueden aplicar si el operador del grupo ofrece comercialmente una parte de los

ingresos de Bitcoin minado o vendido contra el suministro de potencia de procesamiento y los participantes no tienen control sobre los procesos específicos, por ejemplo.

70. BaFin recibe un número creciente de consultas sobre productos derivados y como parecidos a fondos relacionados con Bitcoin. Otra vez, ya que cada caso es diferente, no son necesariamente sujetas a la supervisión. En general, sin embargo, si se negocia comercialmente, estos tipos de productos están sujetas a la supervisión normativa del KWG o la KAGB, porque productos derivados de un instrumento financiero son en sí instrumentos financieros o al menos representan a gestión de activos. La operación comercial de un ATM bitcoin normalmente también es un servicio bancario o financiero sujeto a un requisito de autorización - dependiendo de la forma en que los procesos de compra y las relaciones legales son arreglados entre comprador, vendedor y, en algunos casos - operador.

71. BaFin asume que un negocio se lleva a cabo en Alemania no sólo si el domicilio o residencia habitual del proveedor del servicio domicilio está en Alemania, pero también si se encuentra en el extranjero y el proveedor del servicio se dirige al mercado para repetidamente y comercialmente ofrecer servicios bancarios o financieros a empresas o personas cuyo domicilio o residencia habitual está en Alemania. Sin embargo, esto no afecta la libertad pasiva de prestación de servicios, es decir, el derecho de las personas y empresas residentes en Alemania a pedir los servicios de un proveedor extranjero bajo su propia iniciativa. Por lo tanto, las transacciones que han sido emprendidas porque el cliente ha tomado la iniciativa no requieren autorización del KWG. Para ofertas en línea relativas a los productos del mercado financiero, el criterio relevante es si el análisis del sitio web como un todo revela que los servicios ofrecidos están dirigidos al mercado alemán. Una renuncia es sólo uno de muchos indicadores. Otras indicaciones incluyen el dominio y el dominio de nivel superior, el idioma u otras referencias específicas del país y el marco legal.

72. Los bancos y proveedores de servicios financieros que ya tienen la autorización para comerciar con instrumentos financieros también tienen permitido realizar transacciones con Bitcoin sin estar sujeto a requisitos adicionales de autorización. En todos estos casos la institución autorizada es también una entidad obligada bajo legislación ALA.

HONG KONG, CHINA

73. Hong Kong, China ha adoptado un enfoque muy prudente desde mediados del 2013 en recordar al público los riesgos de consumidor, lavado de activos y cibercrimen asociados a cualquier comercio o negociación con monedas virtuales y materias virtuales, tales como Bitcoin. Hong Kong, China no regula dichas materias virtuales propiamente, ya que no son "moneda", "valores" o "moneda de curso legal" en la legislación vigente. Asimismo, los operadores o concesionarios que prestan servicios en lo referente a materias virtuales no caen dentro de la definición de una "empresa de servicios monetarios" bajo la Ordenanza (para Instituciones Financieras) Antilavado de Activos y Contra la Financiación del Terrorismo, a menos que sus servicios o transacciones implican el cambio de dinero o servicios de remesas. Dicho esto, las instituciones financieras, comerciantes u operadores de materia virtual, o individuos están sujetos a un deber legal para reportar las transacciones sospechosas a la Unidad de Inteligencia Financiera Conjunta, si su trabajo sobre debida diligencia o las transacciones revelan cualquier actividad sospechosa en relación con el

lavado de activos o financiación del terrorismo, independientemente de si están implicadas materias virtuales. La falta de revelar tales transacciones sospechosas puede equivaler a un delito. Las leyes existentes también cubren actos de fraude, delitos de tecnología, esquemas de pirámides o piramidales, el lavado de activos o financiamiento del terrorismo que implican materias virtuales. Además, los reguladores han emitido directrices a las instituciones financieras para recordarles a asegurar un nivel escalado de vigilancia acorde con los riesgos de lavado de activos y financiación del terrorismo asociados con las materias virtuales. Las instituciones financieras han sido recordadas a extremar la prudencia al evaluar los riesgos de lavado de activos o el financiamiento del terrorismo al establecer o mantener relaciones comerciales con clientes y clientes que son operadores de cualesquier esquema o negocio relativos a materias virtuales.

ITALIA

74. En Italia las monedas virtuales no son consideradas moneda de curso legal. En enero de 2015, el Banco de Italia emitió una advertencia sobre el uso de aquellas monedas virtuales llamadas ¹¹ y una comunicación, incluida en el Boletín de Supervisión n.1, 2015, que endorsa a la EBA "Opinión sobre 'monedas virtuales'"; el último desalienta a los bancos y otros intermediarios financieros supervisados contra la compra, tenencia o venta de monedas virtuales. En la misma fecha, la Unidad de Inteligencia Financiera italiana emitió un comunicado sobre la utilización anómala de las monedas virtuales y sobre la detección de transacciones sospechosas de lavado de activos y el financiamiento del terrorismo por las entidades obligadas¹².

RUSIA

75. Conforme al Artículo 27 de la Ley Federal "Sobre el Banco Central de Rusia (Banco de Rusia)", la emisión de sustitutos monetarios está prohibida en la Federación rusa. En enero de 2014 el Banco Central de la Federación de Rusia dio a conocer "Información sobre monedas virtuales, especialmente Bitcoin, utilizado para la realización de transacciones" en su sitio web oficial. El Banco de Rusia advierte a individuos, entidades jurídicas y, fundamentalmente, entidades de crédito y las instituciones financieras no crediticio, contra el uso de monedas virtuales a cambio de bienes, servicios o moneda real en rublos o en moneda extranjera. Debido a la naturaleza anónima de la emisión de monedas virtuales por un número ilimitado de personas y el uso de estas monedas para llevar a cabo las transacciones, individuos y entidades jurídicas pueden involuntariamente ser involucrados en actividades ilegales, incluso LA/FT. Por lo tanto, intercambio de monedas virtuales para moneda real en rublos o en moneda extranjera, así como para bienes y servicios, serán vistos por el Banco de Rusia como implicación potencial de la entidad jurídica en la realización de transacciones sospechosas, especificadas en la legislación vigente de ALA/CFT.

76. Con el fin de mitigar los riesgos de LA/FT asociados con monedas virtuales, el Ministerio de Finanzas, conjuntamente con el banco de Rusia, desarrolló el borrador de ley que impone una prohibición de sustitutos monetarios electrónicos y las transacciones electrónicas de sustitutos monetarios. El Borrador ha sido preparado y se presentará en el Parlamento (Estado Duma).

SINGAPUR

77. En marzo de 2014, la Autoridad Monetaria de Singapur (MAS por sus siglas en inglés) anunció que regulará los intermediarios de MV operando en Singapur para hacer frente a los riesgos potenciales de LA/FT. La MAS introducirá regulaciones que requieren a intermediarios de MV que compran, venden o facilitan el intercambio de MVs para monedas fíat para verificar la identidad del cliente y reportar transacciones sospechosas. Las regulaciones propuestas no abordan la seguridad y la solidez de los intermediarios de MV, ni el correcto funcionamiento de las transacciones de MV.

78. El marco regulatorio propuesto para intermediarios de moneda virtual no ha sido implementado todavía. La intención actual es sólo regular a intermediarios de monedas virtuales que operan en Singapur; es decir, aquellos que tienen una presencia física en el país. Sin embargo, como el espacio de la moneda virtual está evolucionando rápidamente, Singapur seguirá monitoreando de cerca a los enfoques regulatorios tomados hacia monedas virtuales por otras jurisdicciones. Si es necesario, la MAS considerará medidas adicionales para abordar los riesgos que representan las monedas virtuales y sus intermediarios.

SUDÁFRICA

79. La Tesorería Nacional emitió un alerta de usuario al monitoreo de moneda virtual el 18 de septiembre de 2014.¹³ Esta fue una declaración combinada entre la Tesorería Nacional, el Banco de Reserva de Sudáfrica, la Junta de Servicios Financieros, el Servicio de Rentas de Sudáfrica y el Centro de Inteligencia Financiera para advertir a los miembros del público a ser conscientes de los riesgos asociados con el uso de monedas virtuales para transacciones o inversiones.

80. Actualmente en Sudáfrica no hay reglamentos ni leyes específicos que abordan el uso de monedas virtuales. Por lo tanto, no se ofrecen protección legal o recursos a los usuarios de monedas virtuales. Debido a su situación no regulada en Sudáfrica, las monedas virtuales no pueden clasificarse como moneda de curso legal ya que cualquier comerciante puede rechazarlas como un instrumento de pago sin estar en violación de la ley. Las monedas virtuales también no pueden considerarse como un medio de pago ya que no se emiten en la recepción de fondos. Comerciar con monedas virtuales, por lo tanto, se realiza al riesgo del usuario no recurriendo a las autoridades de Sudáfrica. Las autoridades sudafricanas continuarán monitoreando y evaluando el uso de monedas virtuales y consultará con los actores del sector privado en este sentido. Puede emitirse más directrices o regulaciones, si es necesario.

SUIZA

81. En junio de 2014, el Gobierno suizo publicó un estudio y declaración de política sobre la MV *Federal Council Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates*,¹⁴ (el Informe del Consejo Federal sobre Monedas Virtuales en Respuesta a los Postulados de Schwaab (13.3687) y Weibel (13,4070)) que declaró que "el Comercio profesional en monedas virtuales y el funcionamiento de plataformas de comercio en Suiza generalmente están bajo el ámbito de la *Ley Antilavado de Activos*." Entidades dedicadas a estas actividades están obligadas a cumplir "con la obligación de verificar la identidad de la parte contratante y establecer la

identidad del beneficiario final." Al mismo tiempo, la Autoridad Suiza de Supervisión del Mercado Financiero (FINMA) publicó una hoja informativa,¹⁵ haciendo hincapié en que la compra y venta de MV convertible sobre una base comercial y la operación de plataformas de comercio utilizadas para transferir dinero o MV convertible de los usuarios de la plataforma a otros usuarios están sujeta a Ley Antilavado de Activos de Suiza. Antes de comenzar las operaciones, un proveedor de este tipo de servicios debe convertirse en un miembro de una organización de autorregulación (OAR) o aplicar a FINMA para una licencia para operar como un intermediario financiero supervisado directamente (DSFI por sus siglas en inglés). En casos donde actividades comerciales descentralizadas de MV caen bajo la Ley Antilavado de Activos, cumplimiento de las obligaciones de DDC es obligatorio. Dado que MV convertible puede facilitar el anonimato y las transferencias de activos transfronterizos, FINMA considera que comerciar en ella ha aumentado los riesgos de LA/FT, requiriendo DDC estricta, especialmente con respecto a la identificación de cliente. Actividades comerciales que implican MV convertible requieren una licencia bancaria cuando una organización, como parte de sus actividades comerciales, acepta MV convertible de clientes y administran fondos de MV para clientes. Las entidades de MV que obtienen licencias bancarias están sujetas a supervisión prudencial por la FINMA, que supervisará la compañía sobre una base continua para asegurar que cumple con las regulaciones pertinentes. El Consejo Federal sigue monitoreando los desarrollos en el área de MVs para identificar cualquier necesidad de una acción adicional en una etapa temprana.

EL REINO UNIDO

82. Los planes del gobierno británico para las monedas virtuales: en noviembre de 2014, el gobierno del Reino Unido publicó una Convocatoria de Información para recopilar evidencia sobre los beneficios y los riesgos asociados con la monedas virtuales (digitales), con un enfoque particular sobre la cuestión de la regulación. La Convocatoria de Información fue cerrada en diciembre de 2014. En marzo de 2015, el gobierno del Reino Unido publicó un resumen de la evidencia recopilada a través de la Convocatoria de Información y anunció que pretende aplicar regulación de antilavado de activos a los cambios de moneda digital en el Reino Unido. El Gobierno del reino Unido planea consultar formalmente sobre los detalles de la reglamentación propuesta más adelante este año.

83. Los esfuerzos del Reino Unido para mejorar su comprensión de los riesgos con respecto a monedas virtuales: Ha mejorado el nivel de comprensión del riesgo con respecto a MV en el Reino Unido. La Agencia de Crimen Nacional del Reino Unido (NCA por sus siglas en inglés) está liderando una respuesta interinstitucional para evaluar y responder a la amenaza que plantea el uso criminal de las MV, que involucra a la Crown Prosecution Service (Fiscalía de la Corona), HM Revenue and Customs (Ingresos y Aduanas del Su Majestad), Policía de la Ciudad de Londres, HM Treasury (Tesorería de Su Majestad), el Banco de Inglaterra, Autoridad de Conducta Financiera, Home Office y la Metropolitan Police Service (Servicio de Policía Metropolitana).

84. Esta trabajo incluye la construcción de la imagen de la inteligencia. Una evaluación de NCA ha proporcionado una base para el orden público sobre la amenaza que representa el uso criminal de las MV. Una imagen mejorada de inteligencia será la base de objetivos operacionales y también está siendo alimentada a los legisladores para informar la toma de decisiones sobre la intervención del gobierno. Trabajo de desarrollo de capacidades incluyen sensibilización de la industria y las Fuerzas.

Además, gran parte de esta actividad está siendo copiada a nivel internacional, lo cual es importante dada la naturaleza transfronteriza del problema.

LOS ESTADOS UNIDOS

85. Los Estados Unidos regulan cualquier persona natural y jurídica, incluyendo cambiadores y administradores de MV convertible— dedicada a la aceptación y transmisión de MV convertible de una persona a otra persona o ubicación como remitentes de dinero, sujeto a las obligaciones de ALA/CFT, incluyendo registro, identificación del cliente, mantenimiento de registros y requisitos de reporte. La regulación federal de ALA/CFT cubre a tanto las MV convertibles centralizadas y descentralizadas y se aplica a las personas dedicadas a remitir MV convertible en nombre de un tercero sin también cambiar MV de acá para allá por moneda fíat. También se aplica a cambiadores/administradores de MV convertible ubicados en el extranjero que no tienen presencia física en los Estados Unidos, pero que conducen negocios en toda o gran parte en los Estados Unidos. Las vigentes regulaciones de ALA/CFT del gobierno de los E.E.U.U. no se aplican a los usuarios de MV convertible que están usando la MV sin participar en la remisión de dinero. Además de las regulaciones federales, 48 Estados regulan remitentes de dinero, y muchos están considerando cómo puede aplicar su regulación de ALA/CFT y prudencial existente, a los remitentes de dinero a las MV. Por ejemplo, el Departamento de Servicios Financieros de Nueva York (NYFSD por sus siglas en inglés) ha anunciado que pronto emitirá una regulación que le exigirá a algunos negocios de moneda virtual para obtener "bitlicenses" (licencias de bitcoin) y cumplir con las obligaciones de ALA/CFT, normas de revelación del consumidor, requisitos de capital y reglas de inversión.

86. Los Estados Unidos emprendieron cambios legales para acomodar la cambiante tecnología financiera. Reconociendo que las protecciones de ALA/CFT deben estar al tanto con la aparición de nuevos sistemas de pago, en julio de 2011, FinCEN modificó sus reglas con respecto a las Empresas de Servicios Monetarios (MSB por sus siglas en inglés) generalmente¹⁶, proporcionando la flexibilidad necesaria para adaptarse a las innovaciones de los pagos de MV bajo el marco regulador existente de la Ley de Secreto Bancaria (BSA por sus siglas en inglés). La modificada MSB ha añadido la frase, "otro valor que sustituye a la moneda" a la definición de "servicios de remisión de dinero" y así cambió la definición de remitente de dinero MSB. Como resultado de este cambio reglamentario, "servicios de remisión de dinero" se define ahora como "la aceptación de moneda, fondos *u otro valor que sustituye a la moneda* de una persona y la remisión de moneda, fondos *u otro valor que sustituye a la moneda* a otro lugar o persona por cualquier medio"¹⁷. Un "remitente de dinero" es una persona (individuo o entidad) que ofrece servicios de remisión de dinero o cualquier otra persona dedicada a la transferencia de fondos. Dado que "servicios de remisión de dinero," es definido como "la aceptación de moneda, fondos *u otro valor que sustituye a la moneda* de una persona y la remisión de moneda, fondos *u otro valor que sustituye a la moneda* a otro lugar o persona por cualquier medio," los Estados Unidos puede regular a cualquier persona legal o natural dedicada a aceptar MV convertible de una persona y remitirla a otra persona o ubicación, así abarcando, entre otros, cambiadores de moneda virtual convertible y administradores como remitentes de dinero.

NOTAS

- ¹ Por ejemplo, un proveedor de cartera/cambiador/procesor de pagos de un Bitcoin basado en los E.E.U.U., vincula a la cartera de MV del cliente a una cuenta bancaria o tarjeta de cargo o débito tradicional para financiar compras de MV y recibe efectivo de MV. Un servicio de remesas de Bitcoin basado en el Reino Unido en el corredor de Reino Unido-Kenia se vincula a un sistema de pagos móviles kenianos en el punto de entrega. Un cambio de Bitcoin operando en Europa recientemente añadió tarjetas de red de crédito y débito de marca a sus opciones de financiación disponibles, que ya incluía **transferencias bancarias** del Single Euro Payments Area (Área de Pago Unicos de Euro) (SEPA por sus siglas en inglés). Un cambio de Bitcoin con sede en Australia, con clientes en más de 40 países, envía remesas directamente a la cuenta bancaria del beneficiario sin el destinatario usar Bitcoin, pero con el backend de la remesa siendo realizada enteramente en bitcoins.
- ² GAFI (2013), *Directrices para un Enfoque Basado en Riesgo a Tarjetas prepagadas, Pagos Móviles y Servicios de Pago basado en el Internet*, GAFI, París, Francia
www.GAFI-gafi.org/topics/GAFIrecommendations/documents/rba-npps-2013.html
- ³ **Un cambiador de moneda virtual** es una persona o entidad operando como un negocio en el intercambio de moneda virtual para moneda real, fondos u otras formas de moneda virtual y también metales preciosos y viceversa, para un honorario (comisión). Cambiadores generalmente aceptan una amplia gama de pago, incluyendo efectivo, transferencias electrónicas, tarjetas de crédito y otras monedas virtuales y pueden ser afiliados a la administración, no afiliados, o un proveedor tercero. Los cambiadores pueden actuar como una bolsa o como un servicio de cambio. Los individuos suelen utilizar a cambiadores para depositar y retirar dinero de cuentas de moneda virtual.
- ⁴ **Convertible** significa que la moneda virtual puede cambiarse por moneda fiat.
- ⁵ Puesto que MV puede funcionar como un medio de cambio, unidad de cuenta y/o depósito de valor, puede plantear cuestiones a través de un número de jurisdicciones reguladoras complementarias, incluyendo, por ejemplo, regulación de materias primas y valores.
- ⁶ Los Estándares del GAFI constituyen las Recomendaciones de GAFI y sus Notas Interpretativas.
- ⁷ *Definiciones Claves de Monedas Virtuales y los Riesgos Potenciales de ALA/CFT* (GAFI, 2014)
- ⁸ El GAFI define a STDV como servicios financieros que implican la aceptación de dinero en efectivo, cheques, otros instrumentos monetarios u otros depósitos de valor y el pago de una suma correspondiente en efectivo o en otra forma a un beneficiario por medio de una comunicación, mensaje, transferencia, o a través de una red de compensación a la que pertenece el proveedor de STDV. Las transacciones realizadas por dichos servicios pueden involucrar uno o más intermediarios y un pago final a un tercero y **pueden incluir cualquier nuevo método de pago...** [énfasis añadido].
- ⁹ Para una lista completa de las actividades cubiertas por la definición de "instituciones financieras", consulte el Glosario de las *Recomendaciones del GAFI*
- ¹⁰ No bancos en los pagos minoristas, Comité sobre Pagos e Infraestructuras de Mercado, Banco Internacional de Pagos (septiembre de 2014)
- ¹¹ www.bancaditalia.it/compiti/vigilanza/avvisi-pub/index.html
- ¹² http://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf

-
- ¹³ Tesorería Nacional (2014), *Monitoreo de monedas virtuales*, Tesorería Nacional, República de Sudáfrica, disponible en www.treasury.gov.za/comm_media/press/2014
- ¹⁴ Disponible en www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf
- ¹⁵ Disponible en www.finma.ch/e/finma/publikationen/faktenblaetter/Documents/fb-bitcoins-e.pdf
- ¹⁶ *Las Regulaciones de la Ley de Secreto Bancario- Definiciones y Otras Regulaciones Relativas a las Empresas de Servicios Monetarios*, 76 FR 43585 (21 de julio de 2011), 31 CFR § 1010.100(ff)(5)(i)(A) (la Regla de MSB). Casi al mismo tiempo, FinCEN también emitió una nueva Regla Final que aborda el acceso prepago (*Regla Final – Definiciones y Otras Regulaciones Relacionadas con el Acceso Prepagado*, 76 FR 45403 (29 de julio de 2011), 31 CFR § 1010.100(ww)(5)(i)(A) (la regla acceso prepago)).
- ¹⁷ 31 CFR § 1010.100(ff)(5)(i)(A) (énfasis añadido).

APÉNDICE A

MONEDAS VIRTUALES - DEFINICIONES CLAVE Y LOS RIESGOS POTENCIALES DE ALA/CFT ¹

Apéndice A originalmente fue publicado por el GAFI como un documento independiente en junio de 2014

INTRODUCCIÓN

Como las monedas virtuales descentralizada, basada en matemáticas — particularmente Bitcoin ²— han recibido mayor atención, han surgido dos narrativas populares: (1) monedas virtuales son la ola del futuro para los sistemas de pago; y (2) monedas virtuales ofrecen una nueva herramienta poderosa para los delincuentes, financieros terroristas y otros evasores de sanciones para mover y almacenar fondos ilícitos, fuera del alcance del orden público y otras autoridades.³ En este contexto, este documento se fortalece con las Directrices sobre Nuevos Productos y Servicios de Pago (NPPS por sus siglas en inglés) (GAFI, 2013) proponiendo un marco conceptual para comprender y abordar los riesgos de lavado de activos/lucha contra la financiación del terrorismo (ALA/CFT) asociados con una clase de sistema de pago en internet: monedas virtuales. - Específicamente, el documento propone un vocabulario común de definición que aclara qué es la moneda virtual y clasifica los distintos tipos de moneda virtual, basada en sus diferentes modelos de negocio y métodos de operación,⁴ e identifica a los participantes en los sistemas de moneda virtual típica. También aplica los factores de riesgo establecidos en la Sección IV (A) de las Directrices NPPS de 2013 a tipos específicos de monedas virtuales para identificar riesgos potenciales; describe algunas recientes investigaciones y esfuerzos del orden público que implica moneda virtual; y presenta una muestra de los enfoques regulatorios actuales de jurisdicciones a la moneda virtual.

Aunque las Directrices NPPS de 2013 ampliamente aborda los servicios de pago en internet, no definió "moneda digital", "moneda virtual", o "dinero electrónico". Tampoco se centró en monedas virtuales, a diferencia de sistemas de pago en internet que facilitan las transacciones denominados en dinero real (fiat o moneda nacional) (p. ej., Paypal, Alipay o Google Checkout). Tampoco abordó monedas virtuales convertibles descentralizadas, tales como Bitcoin. Las Directrices 2013 también nota que, "[dada la naturaleza en desarrollo de monedas online alternativas, el GAFI puede considerar trabajo adicional en esta área en el futuro" (Directrices NPPS de 2013, p. 11, párr. 29). Un proyecto a corto plazo de tipologías sobre esta base se inició con los siguientes objetivos:

- desarrollar una matriz de riesgo de monedas virtuales (o quizás, más ampliamente, para tanto las monedas virtuales y dinero electrónico);
- promover una comprensión más plena de las partes involucradas en sistemas de moneda virtual convertible y la manera en que la moneda virtual puede ser usada para operar los sistemas de pago; y

- estimular una discusión sobre la implementación de las regulaciones de ALA/CFT basado en riesgo en esta área.

Este proyecto de tipologías puede conducir al desarrollo de una política por el GAFI, por ejemplo, la emisión de Directrices complementarias para la aplicación de un enfoque basado en riesgo a las monedas virtuales que incorporaría el vocabulario propuesto y la matriz de riesgo desarrollado por el proyecto de tipologías y explicaría como específicas Recomendaciones del GAFI aplican en el contexto de moneda virtual.

DEFINICIONES CLAVE:

Un conjunto común de términos que refleja cómo funcionan las monedas virtuales es un primer paso crucial para permitir a funcionarios gubernamentales, de orden público y entidades del sector privado analizar los riesgos potenciales de ALA/CFT de moneda virtual como un nuevo método de pago. A medida que los reguladores y autoridades de orden público alrededor del mundo empiezan a lidiar con los retos planteados por las monedas virtuales, se ha hecho evidente que carecemos de un vocabulario común que refleje de manera precisa las diferentes formas en que se puede presentar la moneda virtual. El siguiente conjunto de términos está diseñado para facilitar la discusión entre los miembros del GAFI. Es importante notar que este vocabulario puede cambiar a medida que la moneda virtual evoluciona y en cuanto los reguladores y funcionarios de orden público/gubernamentales continúan considerar los desafíos que presentan las monedas virtuales. Sin embargo, el vocabulario propuesto pretende proporcionar un lenguaje común para el desarrollo de herramientas conceptuales para ayudarnos a entender mejor cómo funcionan las monedas virtuales y los riesgos y beneficios potenciales que ofrecen.

MONEDA VIRTUAL

Moneda virtual es una representación digital⁵ de valor que puede ser comerciada de manera digital y funciona como (1) un medio de intercambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero no tiene estatus de moneda de curso legal (es decir, cuando se presenta a un acreedor, es una oferta válida y legal de pago)⁶ en cualquier jurisdicción.⁷ No es emitida ni garantizada por cualquier jurisdicción y cumple con las funciones anteriores sólo por acuerdo dentro de la comunidad de usuarios de la moneda virtual. Moneda virtual es distinta de la moneda fíat (también conocido como "**moneda real**," "**dinero real**" o "**moneda nacional**"), que es la moneda de moneda y papel de un país que es designada como su moneda de curso legal; circula; y es habitualmente utilizada y aceptada como un medio de intercambio en el país expedidor. Es distinta al **dinero electrónico**, que es una representación digital de moneda fíat utilizada para transferir electrónicamente el valor denominado en moneda fíat. Dinero electrónico es un mecanismo de transferencia digital para moneda fíat —es decir, electrónicamente transfiere el valor que tiene la condición de moneda de curso legal.

Moneda digital puede significar una representación digital de moneda virtual (no fíat) o dinero electrónico (fíat) y por lo tanto se usa de manera frecuente alternativamente con el término "moneda virtual". En este documento para evitar confusiones, sólo los términos "moneda virtual" o "dinero electrónico" son utilizados.

MONEDA VIRTUAL CONVERTIBLE VERSUS NO CONVERTIBLE

Aunque el documento utiliza "no convertible" y "cerrado", y "convertible" y "abierto" como sinónimos, cabe destacar que la noción de "moneda convertible" no implica en modo alguno una convertibilidad ex officio (por ejemplo, en el caso de patrón de oro), sino más bien una convertibilidad de hecho (por ejemplo porque existe un mercado). Por lo tanto, una moneda virtual es "convertible" sólo mientras que algunos participantes privados hacen ofertas y otros aceptan, puesto que la "convertibilidad" no se garantiza en absoluto por la ley.

Moneda virtual convertible (o abierta) tiene un valor equivalente en moneda real y se puede intercambiar de acá para allá por moneda real. Los ejemplos incluyen: Bitcoin; e-Gold (actualmente paralizado, inactivo o "difunto"); Liberty Reserve (paralizado); Second Life Linden Dollars; y WebMoney.⁸

Moneda virtual no convertible (o cerrado) pretende ser específico a un dominio o mundo virtual particular, como el Massively Multiplayer Online Role-Playing Game (MMORPG) o Amazon.com, y bajo las normas que rigen su uso, no pueden cambiarse por moneda fiat. Ejemplos incluyen: Project Entropia Dollars; Q Coins; y World of Warcraft Gold.

Cabe señalar que incluso donde, bajo los términos establecidos por el administrador, una moneda no convertible es transferible oficialmente solamente dentro de un entorno virtual específico y no es convertible, es posible que un mercado negro no oficial, secundario pueda presentarse que proporcione una oportunidad para el intercambio de la moneda virtual "no convertible" por moneda fiat u otra moneda virtual. Generalmente, el administrador aplicará sanciones (incluso la desafiliación y/o decomiso de moneda virtual restante) para aquellos que buscan crear o utilizar un mercado secundario, contrario a las normas de la moneda.⁹ El desarrollo de un mercado negro secundario sólido en una moneda virtual "no convertible" particular puede, como una cuestión práctica, efectivamente transformarla en una moneda virtual convertible. La característica de no convertible por lo tanto no es necesariamente estática.

MONEDAS VIRTUALES CENTRALIZADAS VERSUS DESCENTRALIZADAS

Todas las monedas virtuales no convertibles están centralizadas: por definición, son emitidas por una autoridad central que establece reglas haciéndolas no convertibles. En cambio, monedas virtuales convertibles pueden ser de dos subtipos: centralizada o descentralizada.

Monedas Virtuales Centralizadas tienen una autoridad única de administración (**administrador**) —es decir, un tercero¹⁰ que controla el sistema. Un administrador emite la moneda; establece las reglas para su uso; mantiene un travesaño central de pagos; y tiene autoridad para redimir la moneda (retirarla de circulación). La tasa de cambio por una moneda virtual convertible puede ser **flotante**—es decir, determinado por la oferta y demanda del mercado de la moneda virtual--o **fija**—es decir, fijado por el administrador en un valor determinado medido en moneda fiat u otro depósito de valor del mundo real, como oro o una canasta de monedas. Actualmente, la mayoría de las transacciones de pagos de moneda virtual implica monedas virtuales centralizadas. Ejemplos: E-gold (paralizado); dólares/euros Liberty Reserve (paralizados); Second Life "Dólares de Linden"; PerfectMoney; WebMoney "Unidades de WM"; y World of Warcraft gold.

Monedas Virtuales Descentralizadas (también conocida como cripto-monedas) son monedas virtuales distribuidas¹¹, de fuentes abiertas, basada en matemáticas persona a persona que no cuentan con un autoridad central de administración y ningún monitoreo o supervisión central. Ejemplos: Bitcoin; LiteCoin; y Ripple.¹²

Cripto-monedas se refiere a una moneda virtual convertible descentralizada, basada en la matemática que está protegida por criptografía. — es decir, incorpora principios de la criptografía para implementar una economía distribuida, descentralizada y segura de información. Cripto-monedas depende de claves públicas y privadas para transferir el valor de una persona (individuo o entidad) a otro y debe ser firmada criptográficamente cada vez que se transfiere. La seguridad, integridad y el balance de ledgers (libros) de cripto-moneda está garantizada por una red de partes mutuamente desconfiadas (en Bitcoin, conocido como los mineros) quienes protegen a la red a cambio de la oportunidad de obtener honorarios distribuidos al azar (en Bitcoin, una pequeña cantidad de bitcoins recién creados, llamados la "block reward (recompensa de bloque)" y en algunos casos, también honorarios de transacción pagados por los usuarios como un incentivo para los mineros incluir sus transacciones en el siguiente bloque). Cientos de especificaciones de cripto-moneda han sido definidas, sobre todo derived from (derivadas de) Bitcoin, que utiliza un sistema de prueba de trabajo para validar las transacciones y mantener la cadena de bloque. Aunque Bitcoin proporcionó el primer protocolo de cripto moneda totalmente implementado, hay interés creciente en el desarrollo de métodos de pruebas alternativas potencialmente más eficientes, tales como los sistemas basados en la prueba de juego.

Bitcoin, lanzado en el 2009, fue la primera moneda virtual convertible descentralizada y la primera cripto-moneda. Bitcoins son unidades de cuenta compuesta de cadenas únicas de números y letras que constituyen unidades de moneda y tienen valor únicamente porque los usuarios están dispuestos a pagar por ellos. Bitcoins se negocian digitalmente entre los usuarios con un alto grado de anonimato y pueden ser intercambiados (comprados o retirados) en dólares estadounidenses, Euros y otras monedas fiat o virtuales. Cualquier persona puede descargar el software gratis y de código abierto de un sitio web para enviar, recibir y almacenar bitcoins y monitorear transacciones de Bitcoin. Los usuarios también pueden obtener direcciones de Bitcoin, que funcionan como cuentas, de un cambiador de Bitcoin o servicio de cartera en línea. Transacciones (flujos de fondo) están disponibles al público en un registro de transacción compartida e identificadas por la dirección Bitcoin, una cadena de letras y números no está sistemáticamente ligada a un individuo. Por lo tanto, Bitcoin se dice que es "pseudo-anónimo". Bitcoin se limita a 21 millones de bitcoins (pero cada unidad puede dividirse en partes más pequeñas), proyectada para ser alcanzado a más tardar 2140.¹³ Hasta el 02 de abril de 2014, habían más de doce y medio millones de bitcoins, con un valor total de poco más de USD 5,5 billones, basado en el índice de cambio promedio en esa fecha.

Altcoin se refiere a una moneda virtual convertible descentralizada basado en matemáticas distinta a bitcoins, la original tal moneda. Ejemplos actuales incluyen Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin y dogecoin. Un popular cambiador, Cryptsy, según la información cambiaría más de 100 diferentes monedas virtuales (hasta el 02 de abril de 2014). (Popper, N., 2013)

Anonymiser (herramienta de Anonimato) se refiere a las herramientas y servicios, tales como acuñado y mezcladores, diseñados para ocultar la fuente de una transacción de Bitcoin y facilitar el anonimato. (Ejemplos: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mezclador)).

Mezclador (servicio de lavandería, tumbador) es un tipo de anonymiser que oscurece la cadena de transacciones en los blockchain mediante la vinculación de todas las transacciones en la misma dirección bitcoin y enviarlas juntas de una manera que les hace parecer como si fueron enviadas desde otra dirección. Una mezclador o tumbador envía las transacciones a través de una serie de transacciones no reales complejas, semi-al azar que se le hace extremadamente difícil vincular monedas virtuales específicas (direcciones) con una transacción determinada. Servicios de mezclador funcionan con el recibo de instrucciones de un usuario para enviar fondos a una dirección bitcoin particular. El servicio de mezclado entonces "mezcla" esta transacción con otras transacciones de usuarios, tal que llega a ser confuso a quien el usuario pretendía enviar los fondos. (Ejemplos: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originalmente, el Onion Router) es una red clandestina de ordenadores distribuida en Internet que oculta las verdaderas direcciones IP y por lo tanto las identidades de los usuarios de red, mediante el enrutamiento de comunicaciones/transacciones a través de múltiples computadoras alrededor del mundo y envolviéndolas en numerosas capas de encriptación. Tor hace muy difícil ubicar físicamente computadoras que acogen o acceden a sitios web en la red. Esta dificultad puede exacerbarse por el uso de tumbadores adicionales o anonymisers en la red Tor. Tor es uno de los varios redes distribuidos clandestinas referidas a menudo como darknets, ciberespacio, el Deep web o redes anónimas, que los individuos utilizan para acceder a contenido en una forma diseñada para ocultar su identidad y actividad de Internet asociada.

Dark wallet (Cartera oscura) es una extensión de cartera basada en navegador, actualmente disponibles en Chrome (y potencialmente en Firefox), que busca garantizar el anonimato de las transacciones de Bitcoin, incorporando las siguientes características: auto-anonymiser (mezclador); comercio descentralizado; uncensurable plataformas de financiación por muchidumbre incensurable; plataformas de bolsa y los mercados negros de información; y los lugares de mercado descentralizadas similares a Silk Road.

Cold Storage (Almacenamiento en frío) se refiere a cartera de Bitcoin fuera de línea —es decir una cartera de Bitcoin que no está conectada al Internet. Cold storage (almacenamiento en frío) pretende proteger a la moneda virtual almacenada contra la piratería y el robo.

Hot Storage (Almacenamiento caliente) se refiere a una cartera bitcoin en línea. Porque está conectada al Internet, hot storage (almacenamiento caliente) es más vulnerable a la piratería/robo que el cold storage (almacenamiento en frío).

Local Exchange Trading System (LETS por sus siglas en inglés)(Sistema Local de Intercambio de Comercio) es una organización económica localmente organizada que permite a los miembros intercambiar bienes y servicios con otros en el grupo. LETS utiliza una moneda local creada para denominar a unidades de valor que pueden ser negociados o truqueadas a cambio de bienes o servicios. Teóricamente, podrían adoptarse bitcoins como la moneda local utilizada dentro de LETS. (Ejemplos: Dólares Ithica; Mazacoin).

PARTICIPANTES DEL SISTEMA DE MONEDA VIRTUAL

Un cambiador (a veces llamado un cambio de moneda virtual) es una persona o entidad dedicado como un negocio en el cambio de moneda virtual por moneda real, fondos u otras formas

de moneda virtual y también metales preciosos y viceversa, por un honorario (comisión). Los cambiadores generalmente aceptan una amplia gama de pago, incluyendo efectivo, transferencias electrónicas, tarjetas de crédito y otras monedas virtuales y pueden ser proveedores afiliados al administrador, no afiliados, o de terceros. Los Cambiadores pueden actuar como una bolsa o como un servicio de cambio. Los individuos suelen utilizar a cambiadores para depositar y retirar dinero de cuentas de moneda virtual.

Un administrador es una persona o entidad dedicada como un negocio en la emisión de (puesta en circulación) moneda virtual centralizada, estableciendo las reglas para su uso; mantenimiento de un libro central de pagos; y quién tiene la autoridad para **redimir** (retirar de la circulación) la moneda virtual.

Un **usuario** es una persona/entidad que obtiene moneda virtual y lo utiliza para comprar bienes o servicios reales o virtuales o envía transferencias a título personal a otra persona (para uso personal), o que mantiene la moneda virtual como una inversión (personal). Los usuarios pueden obtener moneda virtual de varias maneras. Por ejemplo, pueden (1) comprar moneda virtual, usando dinero real (de un cambiador o, para ciertas monedas virtuales centralizadas, directamente del administrador/emisor); (2) participar en actividades específicas que ganan pagos en moneda virtual (por ejemplo, responder a una promoción, completar una encuesta en línea, proporcionar un bien o servicio real o virtual); (3) con algunas monedas virtuales descentralizadas (por ejemplo, Bitcoin), auto-generar unidades de la moneda por "minándolas" (véase definición de minero, abajo) y recibirlas como regalos, recompensas, o como parte de una distribución inicial gratis.

Un **minero** es un individuo o entidad que participa en una red de moneda virtual descentralizada mediante la ejecución de un software especial para resolver algoritmos complejos en un sistema distribuido de prueba de trabajo u otro distribuido de prueba utilizado para validar las transacciones en el sistema de moneda virtual. Los mineros pueden ser usuarios, si auto generan una moneda virtual convertible exclusivamente para sus propios propósitos, por ejemplo, mantener para inversiones o para usarlas para pagar una obligación existente o comprar bienes y servicios. Los mineros también pueden participar en un sistema de moneda virtual como cambiadores, creando la moneda virtual como un negocio para venderla como moneda fiat u otra moneda virtual.

Virtual currency wallet (Cartera de moneda virtual) es un medio (aplicación de software o cualquier otro mecanismo/medio) para mantener, almacenar y transferir bitcoins u otra moneda virtual.

Un proveedor de cartera es una entidad que ofrece una cartera de moneda virtual (es decir, un medio (aplicación de software o cualquier otro mecanismo/medio) para mantener, almacenar y transferir bitcoins u otra moneda virtual). Una cartera contiene las claves privadas del usuario, que permiten al usuario gastar monedas virtuales asignadas a la dirección de la moneda virtual en el blockchain (cadena de bloque). Un proveedor de cartera facilita la participación en un sistema de moneda virtual permitiendo a los usuarios, cambiadores y comerciantes para realizar más fácilmente las transacciones de moneda virtual. El proveedor de cartera mantiene el saldo de moneda virtual del cliente y generalmente también ofrece seguridad de almacenamiento y de transacción. Por ejemplo, más allá de ofrecer direcciones de bitcoin, la cartera puede ofrecer encriptación; protección múltiple de la clave de firma (multiclave), copia de

seguridad/almacenamiento en frío; y mezcladores. Todas carteras de Bitcoin pueden interactuar uno con el otro. Las carteras pueden ser almacenadas tanto en línea ("almacenamiento caliente") o fuera de línea ("almacenamiento en frío"). (Ejemplos: Coinbase; Multibit; Bitcoin Wallet).

Además, varias **otras entidades** pueden participar en un sistema de moneda virtual y pueden estar afiliadas con o independientes de cambiadores o administradores. Estos incluyen **proveedores de servicios de administración de web (también conocidos como administradores de la web); remitentes de pagos de terceros** facilitando la aceptación de los comerciantes; **desarrolladores de software**; y los **proveedores de aplicaciones** (algunas de las "otras entidades" que figuran en este apartado pueden caer ya en una de las categorías anteriores). Las aplicaciones y desarrollo de software pueden ser para fines legítimos —por ejemplo para aumentar la facilidad de aceptación mercantil y pagos de cliente o para responder a las preocupaciones legítimas de privacidad — o para fines ilícitos —por ejemplo un desarrollador/operador de mezcla puede apuntar a los usuarios ilícitos con productos diseñados para evitar el escrutinio regulador y del orden público.

Hay que destacar que esta lista de participantes no es exhaustiva. Además, dado el rápido desarrollo de las tecnologías de moneda virtual y modelos de negocios, participantes adicionales podrían presentarse dentro de los sistemas de moneda virtual y plantear posibles riesgos de ALA/CFT.

Taxonomía de las monedas virtuales

	Centralizadas	Descentralizadas
Convertible	Administrador, cambiadores, usuarios; libros de terceros; pueden ser cambiados por moneda fiat. Ejemplo: WebMoney	Cambiadores, usuarios (no administrador); ningún libro de terceros confiable; pueden ser cambiados por moneda fiat. Ejemplo: Bitcoin
No-convertible	Administrador, cambiadores, usuarios; libros de terceros; no pueden ser canjeados por moneda fiat. Ejemplo: World of Warcraft gold.	No existe

USOS LEGÍTIMOS

Igual que otros nuevos métodos de pago, la moneda virtual tiene usos legítimos, con las firmas de capital riesgoso prominentes invirtiendo en Start-ups de moneda virtual. Moneda virtual tiene el potencial para mejorar la eficiencia de pago y reducir los costos de transacción para pagos y transferencias de fondos. Por ejemplo, Bitcoin funciona como una moneda mundial que puede evitar tasas de cambio, actualmente se procesa con honorarios/cargos más bajos que las tarjetas de débito y de crédito tradicionales y potencialmente puede proporcionar beneficios a los sistemas existentes de pago en línea, tales como Paypal.¹⁴ La moneda virtual también puede facilitar los micro-pagos, permitiendo a las empresas para monetizar mercancías o servicios de bajo costo vendidos en Internet, tales como las descargas únicas de juegos o de música. En la actualidad, como una cuestión práctica, tales objetos no pueden ser vendidos en un costo unitario apropiadamente bajo debido a los costes más altos de transacción asociados con por ejemplo, débito y crédito tradicional. La moneda virtual puede también facilitar las remesas internacionales y apoyar la inclusión financiera de otras maneras, a medida que se desarrollan nuevos productos y servicios a base de moneda virtuales y que potencialmente pueden servir a los menos y no bancarizados. La moneda virtual - en particular, Bitcoin- puede también mantenerse para la inversión. Estos beneficios potenciales deben analizarse cuidadosamente, incluyendo si las supuestas ventajas de costos permanecerán si la moneda virtual cae bajo los requerimientos regulatorios similares a los que se aplican a otros métodos de pagos, y/o si los honorarios por cambio para canjear en moneda fiat se toman en cuenta y si la volatilidad, protección del consumidor y otros factores ¹⁵ limitan su potencial para la inclusión financiera.

RIESGOS POTENCIALES

Las monedas virtuales convertibles que se pueden cambiar por moneda real u otras monedas virtuales son potencialmente vulnerables al abuso de lavado de activos y la financiación terrorista por muchos de los motivos identificados en las Directrices NPPS de 2013. En primer lugar, pueden permitir un mayor anonimato que los métodos tradicionales de pago sin efectivo. Los sistemas de

moneda virtual pueden ser comercializados en Internet, generalmente se caracterizan por relaciones de cliente no cara a cara y pueden permitir financiación anónima (financiación en efectivo o financiación por terceros a través de cambiadores virtuales que no identifican correctamente la fuente del financiamiento). Puede también permitir transferencias anónimas, si el remitente y el destinatario no están adecuadamente identificados.

Los sistemas descentralizados son particularmente vulnerables a los riesgos del anonimato. Por ejemplo, por diseño, direcciones de Bitcoin, que funcionan como cuentas, no tienen ningún nombre u otra identificación de cliente conectado, y el sistema no tiene ningún servidor central o proveedor de servicios. El protocolo de Bitcoin no requiere o proporciona la identificación y verificación de los participantes o genera registros históricos de las transacciones que están necesariamente asociadas con la identidad del mundo real. No hay ningún órgano de supervisión central y no hay software de ALA disponible actualmente para monitorear e identificar patrones de transacciones sospechosas. Las agencias de orden público no puede apuntar a una ubicación o entidad central (administrador) para fines investigativos o de incautación de activos (aunque las autoridades pueden apuntar a cambiadores individuales para la información del cliente que puede recopilar el cambiador). Por lo tanto ofrece un nivel de potencial anonimato imposible con tarjetas de crédito y débito tradicionales o sistemas de pago en línea más viejos, tales como PayPal.

El alcance global de la moneda virtual al igual aumenta sus potenciales riesgos de ALA/CFT. Los sistemas de moneda virtual pueden ser accedidos a través del Internet (incluso a través de los teléfonos móviles) y pueden ser utilizados para hacer los pagos transfronterizos y transferencias de fondos. Además, las monedas virtuales comúnmente dependen de infraestructuras complejas que involucran a varias entidades, a menudo repartidas en varios países, para transferir fondos o ejecutar los pagos. Esta segmentación de servicios significa que la responsabilidad de cumplimiento ALA/CFT y supervisión/ejecución puede ser confusa. Por otra parte, los registros de clientes y transacciones podrán estar en manos de distintas entidades, a menudo en jurisdicciones diferentes, lo que dificulta a las agencias de orden público y los reguladores accederlos. Este problema es exacerbado por la naturaleza rápidamente cambiante de la tecnología de moneda virtual descentralizada y modelos de negocio, incluyendo los cambios de número y tipos/los roles de los participantes que proporcionan servicios en sistemas de pago de moneda virtual. Y sobre todo, los componentes de un sistema de moneda virtual pueden estar ubicados en jurisdicciones que no cuentan con adecuados controles de ALA/CFT. Sistemas de moneda virtual centralizada podrían ser cómplices en el lavado de activos y podrían buscar deliberadamente a jurisdicciones con regímenes débiles de ALA/CFT. Las monedas virtuales convertibles descentralizadas que permiten transacciones de persona a persona de manera anónima, parecen existir en un universo digital totalmente fuera del alcance de cualquier país en particular.

LAS ACCIONES DE LAS AGENCIAS DE ORDEN PÚBLICO INVOLUCRANDO MONEDA VIRTUAL

Las agencias de orden público ya están viendo casos que implican el abuso de moneda virtual para fines de lavado de activos. Los ejemplos incluyen:

LIBERTY RESERVE

En lo que es hasta la fecha el caso de lavado de activos en línea más grande en la historia, en mayo de 2013, el Departamento de Justicia de los Estados Unidos acusó a Liberty Reserve, un remitente de dinero basado en Costa Rica y siete de sus directivos y empleados con la operación de un negocio no registrado de remisión de dinero y el lavado de activos para facilitar el movimiento de más de 6 billones de dólares en activos ilícitos. En una acción coordinada, el Departamento de Tesorería identificó a Liberty Reserve como una institución financiera de preocupación primaria de lavado de activos bajo la Sección 311 de la Ley USA PATRIOT (Acta Patriota), efectivamente cortándolo del sistema financiero de los Estados Unidos.

Establecido en 2006, Liberty Reserve fue diseñado para evitar el escrutinio regulatorio y las agencias de orden público y ayudar a los criminales distribuir, almacenar y lavar los activos del crimen derivados de fraude con tarjetas de crédito, robo de identidad, fraude de inversiones, hacking de computadoras, tráfico de drogas y pornografía infantil permitiéndoles realizar transacciones financieras anónimas y no rastreable. Operando a una escala enorme, tenía más de 1 millón de usuarios en todo el mundo, incluyendo más de 200 000 en los Estados Unidos y manejaba aproximadamente 55 millones de transacciones, casi todos de las cuales eran ilegales. Tenía su propia moneda virtual, Dólares Liberty (LR), pero en cada lado, las transferencias eran denominadas y almacenadas en moneda fiat (Dólares US).

Para utilizar moneda LR, un usuario abría una cuenta a través del sitio Web de Liberty Reserve. Mientras que Liberty Reserve aparentemente requería información básica de identificación, no validaba las identidades. Los usuarios habitualmente establecían cuentas bajo nombres falsos, incluyendo nombres descaradamente criminales ("Russia Hackers," (Hackers de Rusia) "Hacker Account" (Cuenta de Hacker), "Joe Bogus") (Joe falso) y descaradamente falsas direcciones ("123 Fake Main Street, Completely Made up City, New York") (123 Calle Principal Falso, Ciudad Totalmente Falso, Nueva York). Para añadir una capa más del anonimato, Liberty Reserve exigía a los usuarios hacer depósitos y retiros a través de cambiadores terceros recomendados — generalmente, negocios de remisión de dinero sin licencia operando en Rusia y en varios países que no contaban con significativa supervisión o regulación gubernamental de lavado de activos en ese entonces, tales como Malasia, Nigeria y Vietnam. Con la evitación de depósitos y retiros directos de los usuarios, Liberty Reserve eludía la recopilación de información sobre ellos a través de transacciones bancarias u otra actividad que pudiera crear un rastro de papel central. Una vez que se establecía una cuenta, un usuario podría realizar transacciones con otros usuarios de Liberty Reserve con la transferencia de LR desde su cuenta a otros usuarios, incluso "comerciantes" de empresas ficticias que aceptaban los LR como pago. Por un "honorario de privacidad" extra (75 centavos americanos por transacción), los usuarios podían ocultar sus números de cuenta de Liberty Reserve al transferir fondos, así haciendo que las transferencias eran totalmente imposibles de rastrear. Al saber que estaba siendo investigado por las agencias de orden público de los Estados Unidos, Liberty Reserve, pretendió cerrar sus oficinas en Costa Rica pero continuó operando a través de un conjunto de compañías pantallas, moviendo millones a través de sus cuentas en Australia, Chipre, China, Hong Kong, Marruecos, Rusia, España y otros países.¹⁶

SILK ROAD

En septiembre de 2013, el Departamento de Justicia de los Estados Unidos abrió una denuncia penal al presunto dueño y operador de Silk Road, un sitio oculto diseñado para permitir a sus usuarios comprar y vender drogas ilegales, armas, información de identidad robadas y otros bienes y servicios ilegales de forma anónima y fuera del alcance de las agencias de orden público, con el narcotráfico, hacking de computadoras y conspiraciones de lavado de activos. El Departamento de Justicia también incautó el sitio web y aproximadamente 173 991 bitcoins, con un valor de más de 33,6 millones de dólares en el momento de la incautación, desde las computadoras incautadas. El individuo fue detenido en San Francisco en octubre y acusado en febrero de 2014; la investigación está en curso.

Lanzado en enero de 2011, Silk Road funcionaba como un ciber bazar global de mercado negro que intermediaba transacciones criminales anónimas y fue utilizado por varios miles de narcotraficantes y otros vendedores ilegales para distribuir bienes y servicios ilegales a más de cien mil compradores, un tercio de los cuales se cree que estaban en los Estados Unidos. Supuestamente generó un total de ingresos por ventas de aproximadamente 1,2 billones de dólares (más de 9,5 millones de bitcoins) y aproximadamente 80 millones de dólares (más de 600.000 bitcoins) en comisiones para Silk Road. Cientos de millones de dólares fueron lavados mediante estas transacciones ilegales (basadas en el valor del bitcoin en el momento de las fechas de incautación). Las comisiones oscilan entre 8 a 15 por ciento del precio total de venta.

Silk Road alcanzó anonimato mediante la operación en la red oculta de Tor y la aceptación de sólo bitcoins para el pago. La utilización de Bitcoin como la moneda exclusiva en Silk Road le permitió a los compradores y vendedores ocultar más su identidad, ya que los remitentes y los destinatarios de transacciones de bitcoin persona a persona (P2P por sus siglas en inglés) son identificados sólo por la dirección/cuenta de bitcoin anónimo. Además, los usuarios pueden obtener un número ilimitado de direcciones bitcoin y utilizar uno diferente para cada transacción, oscureciendo más el rastro de los activos ilícitos. Los usuarios también pueden emplear adicionales "anonymisers," más allá del servicio de tumbador empleado en las transacciones de Silk Road (ver discusión más abajo).

El sistema de pago de Silk Road funcionaba como un banco interno de Bitcoin, donde cada usuario de Silk Road tenía que tener una cuenta para realizar transacciones en el sitio. Cada usuario de Silk Road tenía al menos una dirección de Silk Road de Bitcoin (y posiblemente miles) asociada (s) a la cuenta de Silk Road del usuario, almacenadas en carteras mantenidas en servidores controlados por Silk Road. Para realizar una compra, un usuario obtenía bitcoins (normalmente a través de un cambiador de Bitcoin) y lo enviaba a una dirección Bitcoin asociada a su cuenta de Silk Road para financiar la cuenta. Cuando se hacía una compra, Silk Road transfería los bitcoins del usuario a una cuenta de fideicomiso que mantenía, en espera de la finalización de la transacción y luego se transfería los bitcoins del usuario/comprador de la cuenta de fideicomiso a la dirección de Bitcoin Silk Road del vendedor. Como un paso adicional, Silk Road empleaba a un "tumbador" para cada compra, que, como explicaba «enviaba todos los pagos a través de una serie compleja, semi-random de transacciones dummy...-lo que hace casi imposible vincular tu pago con cualquier moneda [bits] saliendo del sitio.»¹⁷

WESTERN EXPRESS INTERNATIONAL

Una investigación de ocho años de un grupo ciberdelito multinacional, basado en Internet, El Grupo Western Express Cybercrime, dio lugar a condenas o alegatos de culpable de dieciséis (16) de sus miembros por su rol en un esquema global de robo de identidad/ciberfraude. Los miembros del grupo de cibercrimen interactuaban y se comunicaban principalmente a través de sitios web de “carding” del Internet dedicados al tráfico de tarjetas de crédito robadas e información de identificación personal y utilizaban identidades falsas, cuentas de mensajería instantánea anónimas, cuentas de correo electrónico anónimas y cuentas en moneda virtual anónimas para ocultar la existencia y finalidad de la empresa criminal; evitar la detección por las agencias de orden público y las agencias reguladoras; y mantener su anonimato.

La empresa criminal estaba compuesta de vendedores, compradores, proveedores de servicios de ciberdelincuencia y movers de dinero ubicados en numerosos países, desde Ucrania y en toda Europa Oriental a 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, aceptando pago sobre todo en e-Gold y WebMoney. Los compradores utilizaban las identidades robadas para falsificar tarjetas de crédito y comprar mercancía costosa, que traficaban (incluso vía esquemas de reenvío), cometiendo crímenes adicionales, tales como hurto, posesión criminal de propiedad robada y fraude y generando alrededor de USD 5 millones en activos derivados de fraude de tarjeta de crédito. Los proveedores de servicios de ciberdelincuencia promovieron, facilitaron y ayudaron en la compra, venta y uso fraudulento de números de tarjetas de crédito robadas y otra información de identificación personal por la prestación de servicios de informática a los vendedores y los compradores. El mover de dinero lavaba los activos ilícitos del grupo ciberdelincuente en una gran variedad de formas de alta tecnología, moviendo más de USD 35 millones a través de varias cuentas.

El eje de toda la operación fue Western Express International, Inc., una corporación de Nueva York con sede en Manhattan que funcionaba como cambiador de moneda virtual y remitente de dinero no registrado para coordinar y facilitar las formas de pago de Internet utilizadas por la empresa criminal y para lavar los activos del grupo. Uno de los cambiadores de moneda virtual más grandes en los EEUU, Western Express International cambió un total de USD 15 millones en WebMoney y USD 20 millones en e-Gold para el grupo de ciberdelincuencia y utilizó a bancos y remesadoras 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 las formas de mover dinero de forma anónima y aislarse de los requisitos de reporte.

Western Express International y su dueño/operador, un ciudadano ucraniano, se declaró culpable en febrero de 2013 en el Estado de Nueva York a delitos de lavado de activos, fraude y conspiración. (En febrero de 2006, Western Express fue también acusado de operar un servicio ilegal de canje de cheques/transferencias electrónicas.) Otros tres acusados fueron sentenciados después de juicio en junio de 2013; varios más se declararon culpables en agosto de 2009. Dos acusados ya acusados formalmente permanecen como fugitivos. La investigación fue realizada conjuntamente por el Servicio Secreto de los Estados Unidos y la Fiscalía del distrito de Manhattan (Condado de Nueva York) y fue procesada con éxito por la Fiscalía del distrito de Manhattan.

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 eso todas las delegaciones fueron invitadas a ofrecer comentarios sobre el borrador con miras a adoptar un documento final en la próxima reunión. Se recibieron comentarios de 10 delegaciones, y éstos han sido considerados en la preparación de esta revisión.
- ² "Bitcoin" (en mayúsculas) se refiere tanto al software de código abierto utilizado para crear la moneda virtual y la red de persona a persona (P2P por sus siglas en inglés) formado como resultado de ello; "bitcoin" (minúscula) se refiere a las unidades individuales de la moneda virtual.
- ³ También debe señalarse que algunos observadores, entre ellos el ex Presidente de la Reserva Federal Alan Greenspan, Nout Wellink, un ex Presidente del Banco Central holandés y Ganador del Premio Nobel economista Robert Shiller, sostienen que la moneda virtual es una moda pasajera o burbuja, similar a Tulipmania en los países bajos del siglo XVII.
- ⁴ Moneda virtual es un tema complejo que implica no sólo cuestiones de ALA/CFT, pero también otros temas regulatorios, incluyendo la protección del consumidor, seguridad prudencial, regulación fiscal y de solidez, y estándares de seguridad de la red TI. El vocabulario propuesto es así relevante a través de un número de jurisdicciones reguladoras complementarias. Adopción de términos consistentes y una comprensión conceptual común de moneda virtual por todas las entidades gubernamentales pertinentes es importante para evitar duplicar esfuerzos y/o trabajando en propósitos cruzados no deseados y facilita la capacidad de las autoridades gubernamentales para aprovechar sus diferentes perspectivas y áreas de especialización para identificar más eficazmente y abordar relativas a las monedas virtuales.
- ⁵ **Representación digital** es una representación de algo en la forma de datos digitales—es decir datos informatizados que se representan mediante el uso de valores discretos (discontinuos) para incorporar información, en contraste con señales continuas o analógicas que se comportan de una manera continua o representan la información utilizando una función continua. Un objeto físico, tales como una unidad flash o un bitcoin, puede contener una representación digital de moneda virtual, pero en última instancia, la moneda solo funciona como tal si está vinculada digitalmente, a través de Internet, al sistema de moneda virtual.
- ⁶ Estado de moneda de curso legal no requiere necesariamente a una entidad o individuo a aceptar el pago en un determinado tipo de moneda de curso legal. Por ejemplo, en muchas jurisdicciones, una empresa privada, persona u organización está libre de desarrollar políticas internas sobre si debe o no aceptar la moneda o monedas (efectivo) físicas de la jurisdicción como pago por bienes y/o servicios.
- ⁷ Esta definición difiere del que se ofrece en 2012 por el Banco Central Europeo (BCE), que define moneda virtual "como un tipo de dinero no regulado, digital, que es emitido y generalmente controlado por sus desarrolladores y utilizado y aceptado entre los miembros de una comunidad virtual específica" BCE, *Esquemas de Moneda Virtual* (octubre de 2012), p. 6. El BCE reconoció en la p.13 de su informe que su "definición quizás necesita adaptarse en el futuro si cambian las características fundamentales". Su definición ahora aparece demasiado limitada, puesto que la moneda virtual descentralizada, basada en matemáticas como Bitcoin no son emitidas y controladas por un programador central y algunas jurisdicciones (por ejemplo, los Estados Unidos, Suecia y Tailandia) ahora regulan monedas virtuales.
- ⁸ Por ejemplo, WebMoney es una moneda virtual porque "objetos de valor" (activos) son transferidos y almacenados en forma de una moneda no fiat, las unidades de medida de los derechos de propiedad de

los objetos de valor almacenadas por el garante son Unidades de Título de WebMoney (WM) del tipo correspondiente. <http://wmtransfer.com/eng/about>.

- 9 Por ejemplo, a pesar de las medidas de disuasión, varios cambios permiten la conversión del mercado negro de World of Warcraft Gold.
- 10 Un tercero es un individuo o entidad que participa en una transacción, pero no es uno de los principios y no está afiliado con los otros dos participantes en el transaction—es decir, un tercero funciona como una entidad neutra entre los principales (por ejemplo, remitente y receptor, comprador y vendedor) en un negocio o transacción financiera. La participación de los terceros 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 por menor. Un vendedor ofrece un bien o servicio; un comprador usa una tarjeta de crédito o débito ingresado a través del servicio de pago PayPal; y el tercero de confianza completa a la transferencia financiera. Del mismo modo, en una transacción inmobiliaria, una empresa de depósito de garantía de terceros actúa como un agente neutro entre el comprador y el vendedor, recopilando los documentos del vendedor y el dinero del comprador que los dos principios deben intercambiar para completar la transacción.
- 11 Distribuido es un término de arte que se refiere a una característica esencial de monedas virtuales descentralizadas basadas en matemáticas: las transacciones son validadas por un sistema de prueba de trabajo *distribuido*. Cada transacción *se distribuye* entre una red de participantes quienes ejecutan el algoritmo para validar la transacción.
- 12 Aparte de la creación inicial y la emisión de monedas ripple (RXP), Ripple funciona como una moneda virtual descentralizada. Los fundadores de Ripple crearon todos 100 billones de monedas Ripple y sostuvo 20 billones de ellos, con el resto para ser distribuidos 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 registrado en un libro compartido que es una base de datos constantemente actualizada de cuentas y transacciones de Ripple.
- 13 En 2140, el premio de bloque dejará de estar disponible y los mineros serán recompensados únicamente por los honorarios de transacción.
- 14 Por ejemplo, el PayPal está buscando activamente a aceptar y canjear bitcoins en la plataforma de PayPal, y JP Morgan Chase ha presentado una solicitud de patente de los E.E.U.U. para un sistema de pagos electrónicos en línea utilizando un protocolo de moneda virtual basada en matemáticas que le permitiría a los usuarios realizar pagos anónimos sin proporcionar un número de cuenta o nombre, con la moneda virtual siendo almacenada en los equipos de JPMC y verificados a través de un registro compartido, al igual que la “block chain” (cadena de bloque) en el sistema bitcoin.
- 15 Por ejemplo, queda por verse si sistemas de moneda virtual pueden proporcionar una vía para otros servicios financieros, tales como crédito y de seguros.
- 16 La investigación de Liberty Reserve y desmontaje involucró acciones de parte de agencias de orden público en 18 países y jurisdicciones, entre ellos Costa Rica; los Países Bajos; España; Marruecos; Suecia; Suiza; Chipre; Australia; China; Hong Kong, China; Noruega; Letonia; Luxemburgo; el Reino Unido; Rusia; Canadá; y los Estados Unidos para frenar los activos del crimen, decomisar los nombres de dominio e incautar los servidores.
- 17 La investigación de Silk Road involucró a varias agencias de orden público estadounidenses, llevó a las Operaciones Especiales de Nueva York y División Cibernético de la Oficina Federal de Investigaciones (FBI) y la New York Organized Crime Drug Enforcement Strike Force de la Drug Enforcement Administration (DEA) de Nueva York (integrado por agentes y funcionarios de la DEA, el Servicio de

Ingresos Internos (IRS), el Departamento de Policía de la Ciudad de Nueva York, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), la Policía del Estado de Nueva York, la Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos, el Servicio Secreto de los Estados Unidos, el U.S. Marshals Service, Oficina de Control de Activos Extranjeros (OFAC por sus siglas en inglés y el Departamento de Impuestos de Nueva York), con la asistencia y el apoyo de la oficina de campo de ICE-HIS Chicago, las Secciones de Delitos Informáticos y Propiedad Intelectual y Confiscación de Activos y Lavado de Activos del Departamento de Justicia, la Procuraduría de los Estados Unidos para el Distrito sur de Nueva York y socios de orden público extranjeros, especialmente la Policía Metropolitana de Reikiavik de la República de Islandia y la Oficina Central de la República Francesa para la Lucha Contra Delincuencia Vinculada a Tecnologías de la Información y Comunicación.

BIBLIOGRAFÍA Y FUENTES

GAFI (2013), *GAFI Directrices para un Enfoque Basado en Riesgo para Tarjetas Prepagadas, Pagos Móviles y Servicios de Pago en Internet*, GAFI, París

www.GAFI-gafi.org/topics/GAFIrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealbook*, ("En órbita de Bitcoin: Monedas Virtuales Rivales compiten para la Aceptación", en *New York Times, Dealbook*, (24 de noviembre de 2013,

http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accedido en junio de 2014.

APÉNDICE B

CÓMO FUNCIONA LA MONEDA VIRTUAL CONVERTIBLE DESCENTRALIZADA COMO UN MECANISMO DE PAGOS

INTRODUCCIÓN

1. Bitcoin y otras monedas virtuales convertibles descentralizadas (MV por sus siglas en inglés) ofrecen plataformas de pagos digitales alternativos potencialmente innovadoras. La red Bitcoin en sí fue explícitamente diseñada para servir como un mecanismo electrónico de pago **persona a persona (P2P)**¹ para el comercio en Internet. Pretendía permitir a los usuarios omitir el uso de las instituciones financieras con la transferencia directa de MV una al otra y resolver esas transacciones en casi tiempo real, por lo tanto eliminando los costos de intermediación, tales como costos de transacción y la incertidumbre de pago.

2. **MV descentralizada (también comúnmente referidas como cryptocurrency (criptomoneda))**² es MV convertible distribuida, de código abierto y basada en matemáticas que no implique un "tercero de confianza" para verificar las transacciones y mantener (y conciliar) un libro de transacción. Bitcoin proporcionó el primer protocolo totalmente implementado de cryptocurrency, creando el primer mecanismo de pago de MV descentralizado en el mundo. Posteriormente, cientos de especificaciones cryptocurrency se han definido, en su mayoría derivados de Bitcoin, aunque hay interés constante en el desarrollo de protocolos alternativos, potencialmente más eficientes, utilizando diferentes métodos de prueba³ para validar las transacciones y mantener el libro la contabilidad de transacciones distribuidas en línea.

ALCANCE

3. Este apéndice ofrece una breve explicación de cómo MV convertible descentralizada⁴ funciona como un mecanismo de pagos. Se centra en los aspectos funcionales de las redes de MV convertible descentralizadas, en vez de aspectos técnicos de los protocolos y aborda a **los redes de pagos MV de moneda única**, como Bitcoin, en lugar de plataformas de moneda independiente tales como Ripple.⁵ El documento (1) explica el marco conceptual para MV descentralizada y describe los componentes básicos de una red de pago de moneda única de MV descentralizada; (2) explica paso por paso lo que deben hacer los usuarios para participar en la red Bitcoin y llevar a cabo una transacción; y (3) identifica a muchos de los productos y servicios de pago de MV de terceros (VCPSS por sus siglas en inglés) que han salido recientemente para facilitar el uso de este nuevo mecanismo de pagos. La discusión utiliza a Bitcoin para ilustrar mecanismos de pago de moneda única de MV convertible descentralizada, debido a la ventaja de Bitcoin de ser el primer mover y escala mucho mayor (en términos de número de transacciones y valor y capitalización del mercado), en comparación con otras MVs descentralizadas, y porque hasta la fecha, las inversiones de capital de riesgo e infraestructura en desarrollo para redes de pago de moneda única de MV descentralizadas son abrumadoramente específicas de Bitcoin. Utilizando un ejemplo concreto, en la forma de Bitcoin,

es importante para la claridad descriptiva; no refleja ningún endoso por el GAFI, ni predicción de éxito eventual como un mecanismo de corriente de pagos. Muchos de los términos utilizados en este documento se definen en Monedas Virtuales — Definiciones claves y Riesgos Potenciales de ALA/CFT (junio de 2014 documento de MV) del GAFI, en el **Apéndice A**. Aquellos que no son se presentan en negrita y explican aquí.

MONEDA VIRTUAL DESCENTRALIZADA COMO UNA PLATAFORMA DE PAGOS

MARCO CONCEPTUAL DE MECANISMOS DE PAGOS DE MV DESCENTRALIZADA

4. Sacar a las instituciones financieras de los intermediarios en pagos electrónicos, implica un paso conceptual importante. El protocolo de Bitcoin fue diseñado para replicar varias funciones de fideicomisos que las instituciones financieras realizan típicamente como intermediarios en transacciones electrónicas y de efectivo. Una función fundamental de los fideicomisos es garantizar contra el "gasto doble" y la "falsificación".⁶ **Gasto doble** se refiere a un usuario de MV cediendo titularidad de la MV a una persona y luego cediendo titularidad de la misma MV a otra persona. Surge el problema de gasto doble porque la MV descentralizada existe en la forma de un archivo digital que puede ser fácilmente duplicada y no tiene a alguna autoridad de confianza que mantenga el registro central de las transacciones.

5. Para prevenir el gasto doble y falsificación, Bitcoin depende de un libro de contabilidad pública distribuido en línea, llamado **el blockchain**,⁷ y en la criptografía pública de claves para verificar las transacciones. **Criptografía de clave pública** es un método criptográfico que asigna a un usuario dos claves: **una clave pública y una clave privada**. Una **clave pública (también conocida como dirección de Bitcoin)** es un identificador único que funciona de manera similar a una dirección de correo electrónico para la recepción de correo electrónico y sirve como una cuenta para recibir bitcoins. **Una clave privada** es un código criptográfico que funciona como una contraseña secreta que permite al usuario firmar una transacción MV y transferir los bitcoins a otra dirección. Utilizando la clave privada da prueba de la titularidad de los bitcoins. Cada clave pública/dirección de Bitcoin tiene una clave privada correspondiente. La clave privada está matemáticamente relacionada con la dirección Bitcoin y está diseñada para que la dirección Bitcoin puede calcularse de la clave privada, pero el mismo no se puede hacer al revés, por lo tanto proporcionando seguridad de cuenta y de transacciones. La clave pública debe estar emparejada con la clave privada (firma) para que la MV sea transmitida.

6. El protocolo de Bitcoin requiere que cada transacción sea validada, registrada y revelada⁸ en el blockchain. El **blockchain** funciona como un sistema público de reporte de transacciones. Consiste en **bloques**; cada bloque es una agrupación de transacciones reportadas en orden cronológico. Cuando una transacción se inicia (propuesto), se transmite a la red y los participantes, llamados mineros, ejecutando una pieza especial de software, validan la transacción mediante la resolución de un problema matemático complejo que verifica que los bitcoins en la transacción propuesta ya no ha sido gastado y la añadan al blockchain.⁹ Este mismo proceso de validación distribuida (comunidad), llamada **«extracción»**¹⁰ genera nuevos bitcoins, que son recompensados como pago para el primer minero que resuelve el algoritmo que valida la transacción.¹¹ Se registra cada transacción que se ha llevado a cabo cronológicamente en la blockchain.

PARTICIPANDO EN LA RED BITCOIN PARA ENVIAR Y RECIBIR BITCOINS

7. Originalmente, la red Bitcoin era sólo un sistema de transferencia P2P, sin productos y servicios de terceros. Los usuarios obtenían y almacenaban los bitcoins y realizaban transacciones, ellos mismos. Según lo discutido abajo, la infraestructura de pagos Bitcoin ha evolucionado rápidamente y ahora ofrece una variedad de productos y servicios de pago de terceros para facilitar la obtención, almacenamiento y uso de bitcoins. La siguiente Sección describe los componentes básicos y los pasos necesarios para participar en la red Bitcoin y realizar transacciones de pagos de Bitcoin. La Sección final describe algunas de las entidades que ofrecen servicios y productos de terceros bitcoin.

PARTICIPACIÓN SIN INTERMEDIARIOS

Paso 1: Obtener las Claves Públicas (direcciones), Claves Privadas, y Carteras Necesarias para Participar en la Red Bitcoin.

8. En su forma más básica, para participar en la red Bitcoin *sin intermediarios*, los usuarios descargan e instalan el software gratis de Bitcoin (llamada el “cliente” Bitcoin) a sus computadoras desde un sitio web afiliado. El software de cliente contiene un programa de cartera que genera y almacena pares de claves pública-privada. La clave pública generada por el software se identifica como una dirección única de Bitcoin (una cadena de 24 a 37 caracteres de números y letras), que funciona como una cuenta para recibir pagos de Bitcoin y permitir que un usuario realizar transacciones de Bitcoin. Los usuarios pueden crear/obtener tantas direcciones como ellos quieran. Las claves privadas (con Bitcoin, secuencias aleatorias de 64 letras y números) generadas por y almacenadas en el cliente están vinculadas matemáticamente a una dirección Bitcoin específica. Como una cuestión práctica, las claves privadas **son** la moneda virtual del usuario. El programa de cartera también se comunica con otras direcciones Bitcoin en la red Bitcoin, permitiendo al usuario enviar y recibir bitcoins. El usuario accede a su bitcoin a través de una cartera (un archivo de ordenador) en su ordenador, teléfono móvil u otro dispositivo digital. Alternativamente, los usuarios pueden descargar un software de programa de cartera de un proveedor de carteras en línea tercero. Algunas carteras de software operan en coordinación con el cliente Bitcoin, mientras que otras permiten al usuario evitar descargar el entero cliente Bitcoin sí mismo. Una cartera que el usuario descarga y almacena en su propio ordenador u otro dispositivo digital se llama **“unhosted wallet (una cartera no acogida o sin servidor)”**. El usuario puede almacenar su cartera no acogida en línea (“almacenamiento caliente”) o fuera de línea (“almacenamiento en frío”). Con carteras no acogidas, el dueño es responsable de la seguridad de cartera y proteger las claves privadas.

Paso 2: Obtener Bitcoins

9. Los usuarios pueden obtener bitcoins de varias maneras. Por ejemplo, puede (1) comprar MV de un cambiador tercero, utilizando dinero fiat u otras MV; (2) participar en actividades específicas que ganan los pagos MV (p. ej., responder a una promoción, completar una encuesta en línea, proporcionar un bien o servicio real o virtual); (3) recibirlas como regalos o recompensas; y (4) auto-generar las bitcoins por minería¹², como se describió arriba. La mayor parte de la minería se

concentra ahora en los grupos profesionalizados de minería; los usuarios suelen obtener bitcoins de intercambios terceros.

Tercer paso: Transferencia de Bitcoins

10. Las transacciones de Bitcoin se envían desde y hasta direcciones Bitcoin en carteras Bitcoin y están firmadas digitalmente para la seguridad. Para usar bitcoins para enviar un pago por bienes o servicios o una remesa—es decir, gastar o enviar bitcoins, el usuario utiliza la (s) llave (s) privada (s) para desbloquear su cartera digital y firmar digitalmente la transacción. La transacción en sí contiene tres piezas de información: (1) una entrada (la dirección de bitcoin que fue utilizada *para enviar los bitcoins al remitente actual*); (2) una cantidad (la cantidad de bitcoins que el remitente está transfiriendo); y (3) una salida (la dirección bitcoin del destinatario). Estas funciones automatizadas son manejadas por el software de cartera. El usuario (mediante la descarga del software) envía los bitcoins de su cartera a la red Bitcoin. En ese momento, como se describe arriba, mineros de Bitcoin lo incluyen en un bloque de transacción, verifican la transacción y la entran en el blockchain, confirmando la transacción. La mayoría de las transacciones de Bitcoin que se llevan a cabo por el usuario en sí mismo, sin intermediarios, no tienen honorarios obligatorios. Sin embargo, ahora se recomienda que los usuarios paguen un honorario voluntario para remunerar a los mineros para la confirmación rápida.

Figura 1. Los tres elementos esenciales de una transacción de Bitcoin
(Solo disponible en inglés)

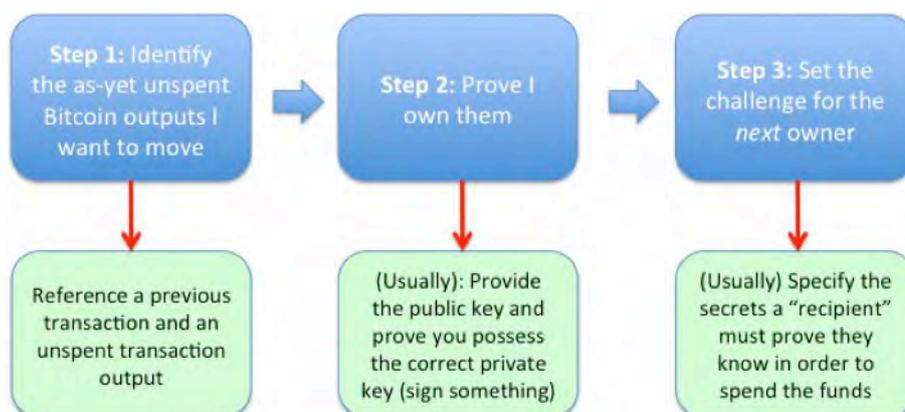


Table courtesy of Bach, A., Corallo, M. Dashjr, L. et al (2014)¹³.

Paso Cuatro: Confirmación

11. Con Bitcoin, anunciando un pago a la dirección del destinatario es casi instantáneo. Sin embargo, la transacción debe todavía ser liada en un bloque por los mineros para comenzar el proceso de confirmación. En promedio, toma aproximadamente 10 minutos para que los mineros en la red Bitcoin a construyan (o resuelven) un bloque determinado. Una vez que una transacción en un bloque ha sido añadida a la blockchain, sigue siendo parte de la blockchain. Todos los bloques

subsecuentes en la blockchain se construyen en la parte superior del bloque que contiene la transacción particular. Cada bloque añadido a la blockchain después de un bloque que contiene una determinada transacción se considera una **confirmación**¹⁴ de esa transacción. Una **confirmación** refleja un consenso en la red que las bitcoins particulares que el destinatario ha recibido no han sido enviadas a más nadie y se consideran propiedad del destinatario. Una transacción debe ser confirmada antes de que el destinatario puede gastar/enviar los bitcoins que ha recibido. Los bloques subsiguientes en el blockchain contruidos en la parte superior del bloque que contiene una transacción particular consolidan el consenso de confirmación y evita la reversión de la transacción. Los usuarios son libres de determinar cuántos bloques subsiguientes, además de la confirmación inicial, se deben agregar a la blockchain antes de que la transacción es suficientemente confirmada que es seguro gastar/transmitir las unidades de MV. Generalmente, una transacción no se considera adecuadamente ser confirmados hasta que un cierto número de confirmaciones (bloques posteriores) — por lo general, seis — aparecen en el blockchain.¹⁵

PARTICIPACIÓN CON LOS INTERMEDIARIOS: INFRAESTRUCTURA DE BITCOIN EMERGENTES

12. Un número creciente de empresas de establecimiento de negocios ha ido surgiendo para proporcionar nuevos productos y servicios de pagos de MV (VCPSS) y que facilitan el uso de redes de pagos de MV descentralizadas, particularmente Bitcoin. En vez de descargar el cliente Bitcoin o una cartera no acogida y almacenar y proteger sus claves privadas y realizar las transacciones ellos mismos, como se describió arriba, los usuarios (consumidores y comerciantes) pueden ahora confiar en una variedad de empresas de terceros que lo hacen mucho más fácil almacenar la MV y realizar transacciones de MV descentralizadas. Existe una gran variedad de modelos de negocio con respecto a estos servicios y productos de terceros. Algunas empresas ofrecen un solo tipo de servicio, mientras que otras ofrecen varios tipos de productos y servicios a sus clientes. Aunque el “ecosistema” de moneda virtual descentralizada está evolucionando rápidamente, a continuación se describen algunos de estos VCPSS terceros.

13. **Proveedor de cartera.** En vez de descargar el software que cree sus propias direcciones, los usuarios ahora pueden obtener direcciones Bitcoin al abrir una cuenta en un cambio de Bitcoin o servicio en línea de cartera. Y en vez de obtener bitcoins de cambiadores y almacenarlos en una cartera no acogida en sus dispositivos digitales, pueden obtener almacenar la MV en una carpeta acogida, proporcionada y asegurado por un **proveedor de cartera**.¹⁶ El proveedor de cartera mantiene el saldo del cliente de moneda virtual y generalmente también proporciona seguridad de almacenamiento y de transacción. Más allá de proporcionar direcciones Bitcoin, el proveedor de cartera puede ofrecer encriptación; múltiple protección de firma de clave (multi clave); copia de seguridad/almacenamiento en frío; y mezcladores. Todas las carteras de Bitcoin pueden interactuar una con la otra. Un proveedor de cartera puede ofrecer almacenamiento bitcoin caliente o fría, con los clientes reteniendo sus claves privadas y control de transferencia de la MV. Alternativamente, el proveedor de cartera puede sostener tanto las claves públicas y privadas para la MV del cliente y la transferencia de MV a terceros en la dirección del cliente, hacer pagos y enviar las remesas. **Muchos cambiadores de MV ofrecen servicios de cartera** (es decir, funcionan también como proveedores de cartera), permitiendo al usuario obtener direcciones y almacenar su MV en una cuenta en el cambio. En la actualidad, predominan dos modelos de carteras de terceros. En la anterior cartera

más 'tradicional' servicios de albergar carteras, el cliente tiene su propia cartera pero el archivo se mantiene en los servidores del servicio de cartera de terceros. (Existen numerosas variaciones de este modelo, particularmente con respecto a si el anfitrión tiene el control total de la (s) clave (s) privada (s)) En el segundo modelo, el que actualmente la mayoría de los cambios están adoptando, los fondos del cliente se mantienen en cuentas combinadas, y la empresa realiza transferencias/retiros según las instrucciones del cliente. Este modelo de negocio permite a más de los fondos de MV ser almacenados en frío, sin afectar el acceso del cliente a su MV.

14. Un procesador de pagos de moneda virtual (también conocido como remitente de pagos de terceros; procesador de pagos mercantil) es una entidad que facilita la aceptación mercantil- es decir, es una entidad que facilita a la transferencia de pagos de moneda virtual de un usuario (cliente) a un comerciante o a otros negocios o profesional que ofrece bienes o servicios de consumo. Por lo general, procesadores de pago ofrecen aplicaciones de software o código incrustable que permiten a la empresa mercantil u otra a aceptar el pago de moneda virtual en su sitio web de Internet o en su lugar de ladrillo y mortero, y que ya sea electrónicamente transmite la moneda virtual a la cartera del comerciante (acogido por el procesador u otro proveedor de cartera, o no acogido y mantenido directamente por el comerciante), o convertir una parte o toda la moneda virtual en moneda fíat y transmitir un pago de dinero electrónico a la cuenta del comerciante, como se indica. Puesto que Bitcoin y otras monedas virtuales convertibles descentralizadas son sistemas de pago basados en Internet diseñados específicamente para eliminar a los intermediarios, puede parecer extraño tener procesadores de moneda virtual como participantes en el ecosistema de moneda virtual. Sin embargo, procesadores intentan hacer más fácil para los negocios comunes, que no son muy técnicos aceptar pagos con moneda virtual. Algunos procesadores de pagos de moneda virtual pueden ofrecer servicios de cambio (conversión) para los comerciantes que aceptan moneda virtual convertible como pago pero temen a potenciales volatilidad negativas de la moneda, permitiéndoles para fines de cobertura inmediatamente convertir moneda virtual entrante en una moneda fíat de su preferencia. Los procesadores también hacen más fáciles para los consumidores (sin muchos conocimientos técnicos) utilizar moneda virtual para comprar bienes y servicios, así ofreciéndoles mayores posibilidades de elección en sus métodos de pagos por menor.

15. Cajero Automático de Bitcoin (también conocido como BTM) se refiere a una máquina automatizada utilizada para el cambio de moneda fíat para bitcoin y/o otra moneda virtual y viceversa. Dependiendo de su funcionalidad programada, las personas pueden usar un ATM bitcoin para comprar bitcoins (y posiblemente otra moneda virtual) (máquinas mono-direccional) o para tanto comprar moneda virtual y canjear moneda virtual para moneda fíat retirando la moneda fíat a cambio de la moneda virtual convertible en el cajero automático (máquinas bidireccional – es decir, canjear/depositar Bitcoin o viceversa). La industria de ATM Bitcoin actualmente está dominada por unos grandes jugadores, pero a medida que crece el sector, otros pueden esperarse entrar. El número de cajeros automáticos de Bitcoin (en vivo) activo es confuso, pero un sitio informa que a hasta finales de noviembre de 2014, habían aproximadamente 300 cajeros automáticos de bitcoin en operación en todo el mundo. Los operadores de ATM Bitcoin cobran una comisión por cada transacción, con algunos fabricantes de ATM Bitcoin ganando una comisión de las tarifas de operación del operador.

NOTA

- ¹ Los pagos de par en par (P2P) son pagos digitales que un usuario envía directamente al destinatario a través de Internet.
- ² En la actualidad, todas las criptomonedas son MV descentralizadas y todas las MV descentralizadas son criptomonedas. Sin embargo, están surgiendo algunas criptomonedas centralizadas (es decir, un sistema centralizado de MV, o incluso un sistema basado en el fiat) que utilizan un libro de contabilidad parecido a una transacción blockchain para manejar las transacciones de clientes. Es posible que en un futuro relativamente próximo, no todas las criptomonedas serán descentralizadas.
- ³ Bitcoin usa un método de prueba de trabajo para verificar las transacciones y crear nuevos bitcoins. Algunos altcoins utilizan pruebas de interés o pruebas de cero conocimiento para este propósito.
- ⁴ Todas las MV descentralizadas son convertibles, por definición (es decir, no existe ninguna autoridad central que establezca los requisitos para la redención).
- ⁵ Hay actualmente dos modelos básicos de mecanismos de pago de moneda virtual descentralizada: redes de MV de moneda única (también conocidos como específicas de moneda), tales como Bitcoin, y redes de MV de moneda independiente, tales como Ripple y Ethereum. Como su nombre indica, **una red de pagos de moneda única** maneja un determinado tipo de moneda virtual descentralizada. **Las plataformas de pago de moneda independiente**, ofrecen una plataforma para transacciones en cualquier moneda virtual o cualquier otro valor negociable, tales como materias primas, acciones, bienes raíces, etc. Para una explicación sobre cómo opera una plataforma de MV de moneda independiente, vea el *Protocolo de Ripple: Un Buceo Profundo para Profesionales de Finanzas*, disponible en <https://ripple.com/ripple-deep-dive/>. Esta citación se proporciona sólo con fines informativos y no representa un aval de GAFI de Ripple o de cualquier otra MV NPPS.
- ⁶ Otra función fiduciaria, normalmente realizada por las instituciones financieras como intermediarios es la garantía de pago de pagador al beneficiario. Para pagos electrónicos tradicionales, instituciones financieras intermedian en transacciones garantizando el pago (es decir, asumiendo el riesgo crediticio del comprador) y ofrecen resolución de controversias post transacción. Bitcoin intenta solucionar el problema de la garantía de pago sin las instituciones financieras logrando liquidación en casi tiempo real y hacer que sus transacciones sean irreversibles (es decir, no sujeto a resolución de controversias).
- ⁷ El **blockchain** es el registro de transacciones de Bitcoin compartido, en la forma de una base de datos públicamente disponible y compartido con un registro secuencial de todas las transacciones.
- ⁸ Todas las transacciones de Bitcoin se almacenan permanentemente y públicamente en el blockchain. Cualquiera que acceda a la red puede ver y monitorear el balance y las transacciones de cualquier dirección Bitcoin, identificadas por clave pública, en el blockchain.
- ⁹ **Mineros**, actuando como nodos en la red, se esfuerzan para "descubrir" el siguiente bloque resolviendo un rompecabezas criptográfico cada vez más difícil, utilizando un algoritmo de hashing. Minería Bitcoin es un proceso puramente matemático, similar a la búsqueda de primer utilizando avanzados **equipos de alto rendimiento**. Mineros de bitcoins buscan para encontrar una secuencia de datos (un "bloque") que produce un determinado patrón cuando el algoritmo de 'hash' Bitcoin se aplica a los datos. El ganador anuncia el nuevo bloque a los otros nodos y recibe nuevos bitcoins como forma de pago. Los otros nodos verifican que la solución cumple con todas las reglas del Protocolo de Bitcoin y luego la aceptan como la próxima entrada oficial en la blockchain, comenzando el proceso nuevamente.
- ¹⁰ **La minería** es el proceso de validación de transacciones distribuidas que genera el blockchain y crea nuevos bitcoins.

- ¹¹ Un minero es otorgado a un número (determinado por el protocolo de Bitcoin) de bitcoins recién creados y en algunos casos, también honorarios de transacción para la resolución de cada algoritmo que sirve para verificar e ingresar los pagos a la blockchain. Un algoritmo lanza nuevos bitcoins en la red en los intervalos preestablecidos--actualmente, 50 cada 10 minutos, con el ritmo reduciendo a la mitad en incrementos de aproximadamente cuatro años hasta más o menos el 2140. En el año 2015, 25 bitcoins se concedieron al minero ganador. Cuando el total de 21 millones de bitcoins está en existencia, el procesamiento de transacciones será recompensado sólo por los costos de transacción. La tasa predeterminada de lanzamiento de la moneda digital pretende asegurar un crecimiento regular de la fuente de dinero Bitcoin a una tasa predecible sin interferencia por parte de terceros, como un banco central, para evitar la hiperinflación.
- ¹² Como se señaló anteriormente, minería involucra la ejecución de una pieza especial de software en sus ordenadores para resolver algoritmos complejos en un "sistema distribuido de prueba-de-trabajo." El usuario es concedido un cierto número de bitcoins recién creados para la solución de cada algoritmo.
- ¹³ Bach, A., Corallo, M. Dashjr, L. et al (2014, *Enabling Blockchain Innovations with Pegged Sidechains*, (October 2014), <https://gandal.wordpress.com/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/>.
- ¹⁴ **Confirmación** se refiere al punto cuando la transacción es validada por un minero y registrada en el blockchain.
- ¹⁵ Aunque algunos comerciantes requieren que los usuarios de MV esperen hasta que la transacción MV está confirmada un número determinado de veces antes de tratar la transacción de pago como pagado y procesar el pedido del cliente, para transacciones de bajo valor, donde el riesgo de fraude no es grande, algunos comerciantes tratan el recibo de bitcoins, en vez de confirmación, como forma de pago válida.
- ¹⁶ **Un proveedor de cartera** es una entidad que ofrece una cartera de moneda virtual para mantener, almacenar y transferir bitcoins u otra moneda virtual.

