ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

18/2014 19 marzo de 2014

David Ramírez Morán

RIESGOS Y REGULACIÓN DE LAS DIVISAS VIRTUALES

RIESGOS Y REGULACIÓN DE LAS DIVISAS VIRTUALES

Resumen:

Los acontecimientos que han afectado a las divisas virtuales durante los primeros meses de 2014 han popularizado la existencia y características de este tipo de activos. Han quedado patentes los riesgos que deben asumir todos los actores que utilizan estos activos, desde los usuarios finales a los negocios que las utilizan. Las autoridades ya han fijado el foco de atención en los riesgos e implicaciones asociadas y se empieza a generar normativa y regulación que permita reducir los riesgos y frenar las actividades ilegales basadas en las características de este tipo de activo.

Abstract:

The issues that have affected the virtual currencies along the first months of 2014 have popularized the existence and characteristics of this kind of actives. The risks that all actors using these actives, from final users to business that use them, have shown clearly. Authorities have focused their attention in the risks and associated implications and are starting a normative and regulative process to lower the risks and stop the illegal activities based on the characteristics of this kind of active.

Palabras clave:

Divisas virtuales, economía, riesgos, legislación, recaudación.

Keywords:

Virtual currencies, economy, risks, regulation, tax collection.

Los acontecimientos que se han producido durante los meses de enero y febrero de 2014 en relación con las divisas electrónicas, y en particular con el servicio de intercambio de Bitcoins Mt. GOX, ha trasladado a toda la sociedad la problemática asociada a este nuevo bien que permite el pago electrónico de bienes y servicios de forma anónima.

Al igual que todo servicio prestado en línea, ha quedado demostrado que nadie está a salvo de la acción de los ciberdelincuentes y que allá donde haya una posibilidad de beneficio, habrá un colectivo detrás con intención de obtenerlo de manera ilícita aprovechando las vulnerabilidades de los sistemas. A este respecto, nadie dentro de la red de funcionamiento de las redes virtuales está exento de riesgos, al igual que ocurre en la economía real, con la diferencia de que la falta de regulación y respaldo deja a los usuarios en una situación de mayor indefensión ante los incidentes.

La oscuridad que caracteriza a estas monedas debido al anonimato que proporcionan ha dado lugar a diversas teorías sobre los hechos acaecidos que serán difícilmente verificables, y menos aún atribuibles a personas u organizaciones concretas, como es habitual en el ciberespacio.

Lo ocurrido no se puede calificar como inesperado porque incluso organizaciones internacionales como el Banco Central Europeo o la Autoridad Bancaria Europea, como se detalla a continuación, ya habían emitido informes y recomendaciones acerca de los riesgos de las divisas virtuales. Las autoridades económicas de los estados, por su parte, también están empezando a tomar cartas en el asunto y se está empezando a generar legislación y normativa que regule la posibilidad de uso de estas divisas en un estado y, dado que se están utilizando para la realización de transacciones comerciales, la aplicabilidad de la legislación existente a estas transacciones.

ADVERTENCIAS DE AUTORIDADES ECONÓMICAS INTERNACIONALES

El Banco Central Europeo público un documento de análisis[1] sobre las características de las divisas virtuales que están invadiendo el ciberespacio y las cabeceras de los periódicos rápidamente. En este informe se trata un primer escollo que consiste en definir los parámetros que caracterizan el dinero y se identificaron tres funciones tradicionalmente asociadas a éste:

[1] ECB, *Virtual currenciesschemes*, Octubre 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Consultado el 18/02/2014]

- Medio de intercambio, como elemento intermediario que facilite la realización de transacciones frente al transporte de bienes para que se encuentren la oferta y la demanda.

- Unidad de cuenta, que constituya una unidad numérica estándar con la que otorgar un valor a los bienes.

- Almacén de valor, que permita ahorrarlo para usarlo en el futuro.

Las principales conclusiones de este informe se resumían en que estas divisas virtuales, que no están denominadas ni respaldadas por divisas reales, no se pueden considerar dinero electrónico de acuerdo a las directivas de la Unión Europea, por lo que no resulta de aplicación la legislación específica. Asimismo, la dificultad para imponer una regulación de las operaciones realizadas con estas divisas y la inexistencia de una entidad que gobierne su evolución se consideran como los principales inconvenientes de su uso por la inseguridad asociada a todas las transacciones y a la evolución de su cotización al cambio con monedas reales. Sin embargo, con el volumen de transacciones actual y el importe asociado a su cotización, a día de hoy no se consideran un riesgo para la estabilidad económica mundial y, sólo en el caso de que se generalice su uso, pueden suponer un problema importante.

La Autoridad Bancaria Europea emitió otro informe[2] el pasado 12 de diciembre de 2013 advirtiendo a la población de los riesgos asociados a la utilización de divisas virtuales. En este informe se destacaban 6 riesgos inherentes al uso de divisas virtuales:

- Perder el importe depositado en las casas de intercambio por no disponer estas de un respaldo económico de los saldos.

- Robo o pérdida del saldo depositado en los monederos digitales por ataques o por la pérdida de las claves o las contraseñas.

- Carecer de protección al utilizarlo como medio de pago.

- El valor de la divisa cambia rápidamente y puede caer hasta un valor nulo.

[2] EBA/WRG/2013/01 *Aviso a los consumidores sobre las monedas virtuales*, 12/12/2013 http://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_ES_TRA1_Vinay.pdf [Consultado 17/03/2014]

- Las transacciones en divisas virtuales pueden respaldar actividades ilícitas o blanqueo de capitales.
- Se puede incurrir en responsabilidades fiscales.

Este informe finalizaba lanzando una advertencia para que los usuarios fueran conscientes de que si recurrían al uso de estas divisas todos los problemas que apareciesen correrían por su cuenta y riesgo, al no resultar de aplicación la regulación de los mercados.

PROPIETARIOS DE BITCOINS

Un factor a tener en cuenta con esta moneda es que en los primeros estadios, cuando el minado de bitcoins estaba al alcance de cualquier ordenador, sólo algunos expertos informáticos estaban dispuestos a dedicar capacidad de sus recursos informáticos al mantenimiento de la red de intercambio en funcionamiento y, simultáneamente, obtener las recompensas. Durante este periodo era muy sencillo conseguir los bitcoins dado que su valor era muy bajo y la cantidad de operaciones para minar un bloque también era bastante reducida. Estos actores iniciales, que tuvieron oportunidad de atesorar un volumen elevado de divisa virtual, pueden ostentar actualmente un elevado poder para controlar la cotización a la que se producen los intercambios, en el caso de que no se hayan ido deshaciendo de sus saldos, lo que deja el control de esta moneda en manos de desconocidos que no tienen por qué tener una formación financiera superior a la de cualquier otra persona.

Cuando empezó a ganar popularidad y la capacidad de procesado del equipo personal empezó a resultar insuficiente, primero se recurrió a la potencia de las tarjetas gráficas que incorporan los ordenadores para multiplicar por 100 la capacidad de minado. Se crearon virus que infectaban los ordenadores para convertirlos en máquinas de minado utilizando bien el procesador o bien tarjeta gráfica. A continuación se recurrió a circuitos basados en dispositivos lógicos programables FPGA, que desbancaban en capacidad de procesado a cualquier otra opción de minado previa. Actualmente, en la carrera por conseguir las recompensas, se han desarrollado circuitos integrados de aplicación específica dedicados al minado con capacidades de cálculo muy elevadas e imbatibles con cualquier otra tecnología, pues se acercan al máximo grado de optimización.

Actualmente, minar Bitcoins mediante ordenadores personales carece de sentido porque su capacidad de cálculo está varios millones de veces por debajo de la que tienen los equipos dedicados actuales basados en circuitos integrados de aplicación específica. Mientras uno de estos equipos puede llegar a hacer varios TeraHashes (10^{12}) por segundo, un ordenador convencional no puede superar el orden de los MegaHashes(10^{6}) por segundo. Es decir, un equipo dedicado tiene un millón de veces más probabilidad de obtener la recompensa por el

minado de un bloque que un ordenador personal particular.

Además de la baja probabilidad de conseguir minar un bloque, la energía necesaria para realizar la cantidad de operaciones que se requiere para minar un bloque en un dispositivo no dedicado supera con creces el valor de la recompensa, por lo que el coste de la electricidad no se vería compensado.

La especialización necesaria para optar a conseguir la recompensa por minado dibuja un escenario en el que los principales mineros se han profesionalizado, aunque no es posible conocer quién se encuentra detrás de estas operaciones. Se pueden identificar dos perfiles interesados en realizar esta actividad. Unos son los especuladores en busca de un puro beneficio económico ante el rápido aumento de la cotización y las grandes posibilidades de operar con los cambios de valor en un mercado muy volátil y carente de regulación. Los otros pueden ser organizaciones dedicadas a actividades ilegales, que se benefician de las características de anonimato que proporcionan las divisas electrónicas para actividades de comercialización de armas, drogas, blanqueo de capitales, pago de servicios fuera del control de los estados, etc.

RIESGOS DERIVADOS DE LAS TECNOLOGÍAS QUE SUSTENTAN LAS DIVISAS VIRTUALES

Las divisas virtuales basan su funcionamiento en algoritmos y en sistemas online que dan lugar a la existencia de riesgos que tanto los usuarios individuales de la moneda como los prestadores de servicios asumen en sus operaciones.

Las divisas virtuales actuales también se denominan criptomonedas porque su funcionamiento se basa en el uso de técnicas de cifrado de clave pública y técnicas numéricas de verificación que requieren una capacidad de cálculo inconmensurable en la actualidad para poder ser contravenidas o falsificadas. La robustez del algoritmo de firma o cifrado es la que da soporte a la seguridad del usuario al evitar que un usuario que conoce sólo una clave pública pueda extraer el valor de la clave privada con la que poder disponer del saldo. A su vez, la verificación numérica que se realiza en el tratamiento de las transacciones asegura que no es posible gastar dos veces la misma moneda o corromper la cadena de bloques que refleja el saldo actualizado de cada usuario de la divisa virtual.

De este modo, existe cierto riesgo tecnológico general para todos los actores que proviene de la posibilidad de que, con el progreso de la capacidad de cálculo o con la aparición de tecnologías disruptivas aplicables como el procesado cuántico, cualquiera de estas dos tecnologías dejen de proporcionar la seguridad que les caracteriza en la actualidad y todo el modelo de funcionamiento de la criptomoneda se desmorone.

Además de los riesgos asociados a la propia tecnología que da soporte a la divisa virtual, su utilización también está sujeta a las vulnerabilidades que tienen los sistemas de información con los que se realizan las transacciones entre los usuarios. Estos riesgos se han analizado desde dos puntos de vista: el correspondiente al usuario final poseedor de cierto saldo y el de los servicios en línea que están surgiendo como intermediarios de las transacciones o para la adquisición, intercambio o venta de divisas virtuales.

Riesgos para los usuarios finales

Cuando un usuario decide utilizar monedas virtuales está asumiendo una colección de riesgos considerable que proviene principalmente de la plataforma tecnológica que utiliza para la realización de las operaciones.

El único dato que debe preservar un usuario es la clave privada asociada a la clave pública contenida en su identificador. En cuanto un atacante tenga acceso a esta clave podrá apropiarse de todo el saldo del usuario mediante una transferencia a otra cuenta de su propiedad. Esta clave se encuentra almacenada en el monedero del usuario, que puede estar ubicado en su propio ordenador o bien ubicarlo en un servicio de intercambio o de gestión de monederos.

Cuando el monedero está en el ordenador del usuario son varias las alternativas por las que un atacante se puede hacer con las claves del usuario. La forma más sencilla consiste en acceder al fichero del disco duro en el que se encuentran ubicadas las claves. Una de las implementaciones más importantes de Bitcoin almacena en el directorio del programa un fichero wallet.dat que contiene todos los datos del monedero y que resulta fácilmente localizable e interpretable.

La opción de cambiar el nombre al fichero también ha sido considerada por los atacantes y existen virus que van analizando la memoria y el disco duro del ordenador en busca de las claves públicas. Esta tarea es relativamente sencilla dado que el identificador, como se detallaba en el artículo anterior, empieza por 1 ó 3 e incluye un valor de comprobación que permite validar fácilmente una cadena de caracteres como identificador. En caso de serlo, la naturaleza de código abierto del software permite determinar con facilidad la ubicación de la clave privada correspondiente. Por tanto, en poco tiempo es posible analizar toda la memoria y el disco duro del ordenador hasta localizar las posibles claves almacenadas.

Para proteger al usuario de estos riesgos existen varias alternativas. La más simple es ubicar los ficheros con las claves en un dispositivo de memoria externo como un pendrive o una tarjeta de memoria que sólo se conecta al ordenador para hacer una transacción y luego vuelve a desconectarse. De esta forma se reduce el intervalo de vulnerabilidad, aunque no

se puede despreciar el riesgo de que los atacantes modifiquen el código del monedero para acceder a los datos justo cuando se va a realizar una transacción.

Otra alternativa consiste en cifrar el fichero almacenado en el disco duro con una contraseña que haya que introducir cada vez que se desee hacer una transacción. Al igual que en el caso anterior, si los atacantes consiguen acceder a los datos y a la contraseña, podrán hacerse con las claves.

Perder las claves es tan nefasto como que terceras personas puedan tener acceso a ellas. Si un usuario pierde su clave privada, no hay forma de poder acceder al saldo asociado a ese identificador y queda bloqueado para siempre. Esto, que podría parecer poco probable, se puede producir si, por ejemplo, se estropea el pendrive en el que se almacenan las claves, falla el disco duro, desparece el fichero fruto de un borrado accidental o un virus o si, en una de las habituales reinstalaciones del sistema operativo, se olvida hacer copia de seguridad del fichero.

Si, por el contrario, se utiliza un servicio de monedero online, las claves del usuario, en caso de existir según haya o no un monedero asociado al usuario, se encuentran almacenadas en los servidores de los prestadores del servicio y no hay posibilidad de robo aunque, pese a eliminar parte de los riesgos anteriores, surgen otros nuevos riesgos. Mediante phishing, un atacante puede falsificar la página web en la que se realizan las transacciones y conseguir los datos de usuario y contraseña en la página web. Con un keylogger, que registra las pulsaciones de teclado, también es posible conseguir este objetivo.Con estos datos el atacante puede ordenar operaciones en nombre del usuario y transferir el saldo. Además, la solución que están utilizando los bancos para evitar estos riesgos, como enviar un SMS a un móvil con una clave o remitir por correo una tarjeta de coordenadas, no son de fácil aplicación en el caso de las divisas virtuales pues se perdería la anonimidad que caracteriza a las mismas.

En los monederos online toda la confianza se está depositando en el prestador del servicio, que en todo momento tiene o puede tener acceso a las claves del usuario, por lo que podría hacer una transferencia del saldo del usuario y no habría posibilidad de recuperarlo. Después, la compañía podría denunciar un ataque de terceras personas a sus servidores y embolsarse los fondos de sus usuarios.

Riesgos para los prestadores de servicios

Los servicios de intercambio también se encuentran expuestos a ataques de diversos tipos. En primer lugar, los ataques señalados anteriormente de phishing o keyloggers pueden suponer un riesgo para la credibilidad del sitio debido a la facilidad con la que un usuario

desencantado puede difundir una mala imagen de un servicio que se basa fundamentalmente en la confianza que el usuario deposita en el prestador.

Como en todo servicio online, existe también la posibilidad de los ataques habituales como la denegación de servicio distribuida o la búsqueda de vulnerabilidades en los portales web con los que se prestan los servicios a los usuarios, para acceder a los sistemas, a los monederos, a los datos de los usuarios, etc.

La implementación que el prestador realiza de los algoritmos también es muy importante. Recientemente se ha seguido en la prensa la evolución del caso de Mt. GOX, un servicio de intercambio radicado en Japón cuya implementación permitía a los usuarios duplicar las operaciones con cargo al saldo de bitcoins de la compañía. El servicio de reclamaciones recibía quejas por operaciones que supuestamente no se habían realizado pero que en la práctica sí se habían hecho. Debido a un fallo de implementación de la comprobación de si una transacción ya se había completado, denominado maleabilidad de las transacciones, la operación volvía a realizarse, por lo que se transfería la misma cantidad dos veces a la cuenta de destino. Esto, combinado con el rápido aumento de la cotización de la divisa virtual, ha conducido a la compañía a la declaración de bancarrota bajo la legislación de Japón[3] y, posteriormente, al amparo del capítulo de la Ley de Bancarrotas estadounidense[4].

Otro riesgo radica en la posibilidad de que los atacantes consigan acceder a las claves de las cuentas de los prestadores de los servicios, como ha ocurrido en el caso de Flexcoin. Esta compañía mantenía dos cuentas para su operación: una primera con el grueso del saldo en poder de la compañía almacenada de forma segura, y una segunda con un saldo menor con la que realizaba todas las operaciones solicitadas por los usuarios. Pese a esta medida de seguridad, la vulneración de la cuenta de liquidez de la empresa ha supuesto un impacto económico tal que ha llevado a la compañía a la quiebra[5].

RESILIENCIA DE LA DIVISA VIRTUAL

Los problemas de Mt. GOX han supuesto un descalabro de la cotización de la divisa virtual en las operaciones realizadas por este proveedor debido al pánico que se generalizó

[3] EFE. *Mt.Gox se declara en quiebra tras anunciar la desaparición masiva de bitcoins*, 28/02/2014 http://www.efe.com/efe/noticias/america/economia/gox-declara-quiebra-tras-anunciar-desaparicion-masiva-bitcoins/2/11/2252514 [Consultado 18/03/2014]

[4] El economista. *La plataforma de intercambio de bitcoin Mt. Gox solicita la bancarrota en EEUU, 10/03/2014* http://www.eleconomista.es/mercados-cotizaciones/noticias/5607517/03/14/La-plataforma-de-intercambio-de-bitcoin-Mt-Gox-solicita-la-bancarrota-en-EEUU.html [Consultado 18/03/2014]

[5] Reuters. *Bitcoin bank Flexcoin shuts down after theft,*04/03/2014http://www.reuters.com/article/2014/03/04/us-bitcoin-flexcoin-idUSBREA2329B20140304 [Consultado 18/03/2014]

rápidamente entre sus usuarios. Las cotizaciones de la divisa en el resto de operadores que permiten el cambio entre moneda real y divisa virtual, pese a haber experimentado caídas importantes, se desligaron de la tasa de cambio de Mt. GOX tan pronto como salieron a la luz las verdaderas causas de los problemas: la maleabilidad de las transacciones que permitía el software que utilizaba el operador. Es decir, pese a haberse producido en un primer momento una caída generalizada de las cotizaciones ante la incertidumbre de que los algoritmos fueran vulnerables a un ataque, al determinar que sólo se trataba de un problema del operador, el mercado frenó la sangría en los operadores no afectados. Este comportamiento se puede asociar a la existencia de una confianza en la fortaleza de la moneda, cuya cotización, una vez identificados y compartimentados los problemas, ha visto reducida su volatilidad a valores más acordes con los que han venido caracterizando su evolución.

MERCADOS EN BITCOINS

Alrededor de las divisas virtuales se está creando todo un mercado que presenta oportunidades de negocio para distintos actores. Las casas de intercambio, los cajeros de bitcoins y las tiendas y servicios que permiten el pago con divisas electrónicas se están generalizando.

En paralelo, las autoridades empiezan a ganar consciencia de las consecuencias fiscales que puede acarrear el uso de divisas virtuales frente a monedas reales y están trabajando en la regulación y fiscalización de este mercado para evitar la evasión fiscal y la facilidad con la que estas divisas permiten el blanqueo de capitales.

Casas de intercambio y depósito

Una casa de cambio a todos los efectos realiza las mismas operaciones que un banco aunque con dos diferencias muy importantes. La actividad que realiza no está regulada ni respaldada por organismos que velen por el funcionamiento transparente y en iguales condiciones para todos los usuarios y, en caso de surgir problemas, el saldo de los usuarios no está respaldado por ningún estado u organización, existiendo el riesgo de perder completamente la inversión.

Estos negocios proporcionan un entorno más amigable para los usuarios gracias a que no es necesario instalar ningún software en su ordenador ni acceder directamente a las redes que dan soporte al funcionamiento de la divisa virtual.

El modelo de negocio de estas casas de intercambio se basa fundamentalmente en la aplicación de una comisión en las transacciones con un importe por debajo del 1% de la

operación realizada. Los costes asociados son mucho menores que los que corresponderían a una operación equivalente realizada en los mercados tradicionales, especialmente si se consideran las operaciones internacionales de movimiento de fondos.

Comercio de bienes

Cada vez aumenta más el número de tiendas que permiten el pago de los bienes que proporcionan mediante divisas virtuales como bitcoin. Estas tiendas tienen una gran importancia porque también permiten establecer un vínculo entre la divisa virtual y el mundo real, al permitir obtener bienes reales a cambio de estas divisas. Constituyen una alternativa a los servicios de intercambio, en los que se pueden vender divisas virtuales a cambio de moneda real.

Las primeras tiendas que aceptaron el pago con divisas virtuales estaban relacionadas con actividades ilícitas, como la compra de drogas, armamento y otras actividades constitutivas de delito en la mayor parte de las legislaciones. La anonimidad que se obtiene con el uso de la divisa virtual en combinación con las tecnologías de anonimización existentes proporciona un mecanismo de compraventa que dificulta o incluso imposibilita la atribución de estas operaciones a las personas que las llevan a cabo. En la prensa se publicó el caso de Silk Road, una página web en la que se comerciaba con sustancias, servicios y objetos prohibidos y que fue desmantelada por el FBI en 2013[6].

El uso creciente de estas divisas virtuales está haciendo que empresas de productos de consumo estén empezando a aceptarlas como medio de pago para adquirir productos como billetes de viaje o material electrónico. El envío de los productos a una dirección física o la necesidad de proporcionar los datos del viajero constituyen una pérdida completa de la anonimidad de la transacción y, haciendo un análisis previo de las transacciones del identificador con el que se hace el pago, de las posibles actividades desarrolladas por el comprador.

Actualmente, están surgiendo páginas web que permiten localizar con facilidad empresas que aceptan el pago de sus productos o servicios con Bitcoin.

Los comerciantes que adoptan la posibilidad de pago con divisas virtuales se exponen a una caída de la cotización que no permita cubrir los costes de los productos servidos aunque, manteniendo un saldo limitado mediante el cambio periódico de divisas virtuales a dinero real, este riesgo se puede mantener controlado. Otra alternativa consiste en que la empresa

[6] *Silk Road underground market closed – but others will replace it* The Guardian, 3/10/2013 http://www.theguardian.com/technology/2013/oct/03/silk-road-underground-market-closed-bitcoin [Consultado 18/03/2014]

utilice los fondos recaudados en divisa virtual para adquirir más bienes para su comercialización, con la posibilidad de realizar un pago libre de impuestos por la adquisición de las mercancías a falta de regulación normativa.

Cajeros automáticos

Son muchas las ciudades en todo el globo en las que se han instalado cajeros automáticos con diferentes opciones de funcionamiento. Hay tres tipos de cajero, según permita comprar la divisa virtual, realizar transferencias con ella o, directamente, recuperar la inversión mediante la venta de los bitcoins a cambio de dinero en metálico. El primer y el segundo caso suponen operaciones de bajo riesgo y consecuencias limitadas. Sin embargo, el tercer caso es más complejo dado que permite la realización de prácticas ilegales relacionadas con el flujo ilícito de capitales y el lavado de dinero negro. Uno de los fabricantes de cajeros que proporciona este servicio solicita los datos del DNI y la huella de la mano del cliente para que la operación de venta de Bitcoins se pueda llevar a cabo. Además de las medidas de identificación, en aquellos lugares donde se ha instalado esta clase de cajeros automáticos se han fijado límites bastante bajos al volumen máximo de las operaciones de venta de Bitcoins que puede realizar una misma persona.

El primer cajero automático de Bitcoins se instaló en Chipre en plena crisis financiera[7]. España no se ha quedado atrás y también se ha instalado un cajero automático en Barcelona, que sólo permitía la adquisición de la divisa virtual[8]. Otros ejemplos de la instalación de cajeros por el mundo se han dado en Irlanda, Corea del Sur, etc.

Estos dispositivos constituyen una herramienta que puede conducir a una mayor popularización de las divisas virtuales, pues acercan al ciudadano medio la posibilidad de adquirir la divisa con gran facilidad y de forma anónima.

Incautación de bitcoin

Son ya varios los casos en los que las autoridades han conseguido desmantelar actividades ilegales que utilizaban las divisas virtuales para conseguir el anonimato de los usuarios. El caso más destacado es la tienda de sustancias ilegales, drogas y armas Silk Road. En esta operación, el FBI se incautó además de un saldo bastante elevado de bitcoins, que era la moneda utilizada para el pago de los productos y servicios ofertados en la página web.

[7] *El primer cajero automático de Bitcoin será instalado en Chipre*, http://alt1040.com/2013/03/cajero-automatico-de-bitcoin[Consultado 17/03/2014]

[8] *Barcelona acoge el primer cajero de bitcoins en España*. Expansión 26/02/2014 http://www.expansion.com/2014/02/26/mercados/1393414929.html [Consultado 18/03/2014]

En España también se ha producido la incautación de un volumen considerable de bitcoin en la operación Ransom, que derribó la organización que se valía del uso del conocido como "virus de la policía" para extorsionar a los dueños de los ordenadores infectados[9].

Estas incautaciones suponen un problema porque requieren una actuación rápida por parte de las autoridades para conseguir acceder a las claves de los monederos en los que se encuentran depositados los saldos, y para establecer un mecanismo de incautación efectivo. Para ello, las autoridades cuentan con monederos de bitcoin con los que, una vez recibida autorización judicial, se transfiere el saldo y permiten, posteriormente, convertir la divisa virtual en moneda de curso legal que depositar en cuentas bancarias de consignaciones judiciales para que el procedimiento siga el curso de la justicia.

La operación de venta de la divisa electrónica conlleva complicaciones por varios motivos. La volatilidad de la cotización de las divisas virtuales puede dar lugar a que el demandado, si no se demuestra su culpabilidad, requiera la devolución de sus divisas virtuales, y en el caso de aumento de su cotización puede dar lugar a situaciones de lucro cesante.

En el caso de Silk Road, el elevado volumen incautado dificulta la venta de la divisa virtual sin que se produzcan efectos en la cotización. En ese caso, el volumen incautado ascendía a cerca del 6% de la divisa en circulación, por lo que una venta indiscriminada hubiera supuesto una rápida caída de la cotización. Este efecto tampoco es deseable porque disminuye el valor del activo incautado, con lo que se reduce el saldo disponible para satisfacer multas o compensaciones por la actividad ilícita o ilegal desarrollada por el procesado.

Regulación de los estados

La regulación por parte de los estados respecto al uso de las divisas electrónicas es muy variada, incluso en entornos que cabría considerar uniformes como la Unión Europea.

Las decisiones tomadas van desde la prohibición absoluta de su uso, como en el caso de Rusia o Indonesia, hasta la consideración como activo financiero que no está sujeto a impuestos por su cambio y circulación, como es el caso del Reino Unido.

[9] Así se incauta la Policía de Bitcoins. Diario El Mundo, 01/11/2013, http://www.elmundo.es/tecnologia/2013/11/01/5270d45363fd3da7618b4576.html [Consultado 18/03/2014]

El documento emitido por las autoridades del Reino Unido[10] resulta de gran interés porque expone claramente los motivos que han conducido a las decisiones tomadas, que consisten en la exención de impuestos por el tráfico, el almacenamiento o los beneficios obtenidos con la divisa virtual y, como única excepción, se detalla la obligatoriedad de satisfacer los impuestos de valor añadido por parte de los comerciantes incluso en las transacciones realizadas en divisas virtuales.

El informe publicado por la Biblioteca del Congreso de Estados Unidos constituye un documento de referencia sobre la situación actual de la moneda en un gran número de países. En este informe se incluye la situación de España haciendo referencia al documento publicado por un abogado español en su página web[11] donde se desgrana la aplicabilidad de la legislación nacional a las divisas virtuales.

El problema que ha ocurrido con Mt. GOX supone un referente de gran importancia porque ante la materialización de un riesgo de la divisa virtual, la caída de una casa de intercambio, el problema ha desbordado en la economía real. La empresa, al encontrarse en quiebra técnica, ha solicitado la declaración de bancarrota ante las autoridades japonesas y estadounidenses para paliar las consecuencias penales que podrían resultar de aplicación al propietario del negocio. La conmoción que se ha producido en los mercados y la notoriedad pública que ha alcanzado el hecho se pueden identificar como los detonantes de la investigación que se ha puesto en marcha por parte de las autoridades japonesas y estadounidenses para analizar lo que ha ocurrido con la casa de intercambio.

CONCLUSIONES

Las divisas virtuales presentan unos riesgos que han quedado más que demostrados por los acontecimientos ocurridos durante los primeros meses de 2014. Estos riesgos se encuentran identificados por los principales organismos internacionales. Sin embargo, la voluntad de los usuarios de seguir utilizando la divisa virtual, respaldada por las numerosas transacciones que se llevan a cabo cada día, da muestras del riesgo que están dispuestos a asumir los actores para ocultar sus intercambios financieros.

---

[10] *Tax treatment of activities involving Bitcoin and other similar cryptocurrencies*, Revenue & Customs Brief 09/14,http://www.hmrc.gov.uk/briefs/vat/brief0914.htm [Consultado 16/03/2014]

[11] Pablo Fernández Burgueño, *12 cosas que deberías saber antes de usar bitcoins (La Ley y el Bitcoin),* http://www.abanlex.com/2013/11/12-cosas-que-deberias-saber-antes-de-usar-bitcoins/ [Consultado 16/03/2014]

La evolución de la cotización de la moneda tras el descalabro sufrido con la caída de Mt. GOX se puede interpretar como una muestra clara de la resiliencia de la moneda. Pese a las consecuencias que va a suponer para los que eran usuarios de Mt. GOX y que han perdido sus fondos, la divisa virtual ha superado el trance y sigue en funcionamiento.

El ataque a una de las plataformas que da sustento a las actividades ilegales que se pueden realizar en la red redunda en la vulnerabilidad a la que están expuestos absolutamente todos los actores que desarrollan sus actividades en la red. Estos ataques cada vez tienen mayores consecuencias y es necesario que los estados se doten de las herramientas necesarias para reducir los riesgos y para poder luchar contra los delincuentes en su búsqueda de oportunidades de enriquecimiento ilegal.

La evolución que espera a las divisas virtuales no presenta un futuro predecible, aunque las acciones que están tomando los estados y organizaciones internacionales denotan una clara tendencia a regular las operaciones relacionadas con este tipo de activos para reducir el riesgo asociado a su uso y para prevenir la escalada de actividades ilegales respaldadas por estas divisas como son la evasión fiscal y el blanqueo de capitales.

David Ramírez Morán
Analista del IEEE