APM 3.9.

Publicación digital. - Asociación Profesional de la Magistratura

JULIÁN GARCÍA MARCOS

PAÍS VASCO

INVESTIGACION DEL FRAUDE CON BITCOINS EN FUENTES ABIERTAS Y COLABORACION DE TERCEROS

La reciente **Sentencia nº 326/2019 de 20 de Junio (Ponente: Don Pablo Llarena Conde) de la Sala de lo Penal del Tribunal Supremo** tuvo la ocasión de pronunciarse, quizá por primera vez en el ámbito penal, al respecto de la perpetración de un delito directamente relacionada con ***bitcoin* y la tecnología *blockchain***. Analizaba, entre otros aspectos, la apariencia ilícita de un negocio consistente en gestionar *bitcoins* de distintos clientes con la finalidad de reinvertir los dividendos obtenidos en la inversión y entregar, al vencimiento del contrato, las ganancias obtenidas. Si bien es cierto que la Sentencia, apenas, ahonda en el aspecto tecnológico de la cuestión sí que tiene la oportunidad, por primera vez, de referirse a los ***bitcoin* como "objeto" de restitución** aseverando, no sin cierta inexactitud[1], que el bitcoin no es sino un "*activo patrimonial inmaterial, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica bitcoin*".

Lo cierto es que, desde hace prácticamente una década, *bitcoin* es una realidad que, si bien ha tenido relevante trascendencia en el ámbito monetario o tributario, apenas ha contado con proyección en el ámbito penal. Y ello aun cuando el propio **Banco Central Europeo, en el año 2012**, lo definiera como "*clase de dinero digital no regulado, emitido y habitualmente controlado por sus desarrolladores y que se usa y acepta entre los miembros de una Comunidad virtual*" reconociéndosele, desde un principio, y, al menos,

1 .- Resulta interesante, en este sentido, la lectura de articulos de publicaciones especializadas en la materia tales como https://www.xataka.com/criptomonedas/bitcoin-no-tiene-consideracion-legal-dinero-confirma-tribunal-supremo .

desde un punto de vista económico, la cualidad de "moneda" pues el *bitcoin* constituye un depósito de valor (su acumulación determina capacidad adquisitiva) , es un medio de pago y una unidad de cuenta lo cual, a priori, convierte al **bitcoin en un elemento objetivo apto para ser objeto de estafa, distracción o ilícita apropiación** y que, tradicionalmente, desde muchos sectores de la economía y el derecho, se haya relacionado al *bitcoin* con el blanqueo de capitales o la venta ilegal de contenidos a través de Internet.

En este último sentido, recientemente han sido noticia grandes operaciones contra **mercados que operan en la "*dark web*"** y cuyo objeto era la venta ilegal de drogas o armas. En marzo de este mismo año DreamMarket, uno de estos potentes mercados, anunció que transfería sus servicios a otra dirección de la web justo el día anterior a que FBI, Europol y la DEA anunciaran múltiples detenciones por tráfico de drogas presuntamente cometidos a través de la citada web[2] y poco después, quien venía llamado a ser su sustituto, Wall Street Market también echaba el cierre siendo que sus administradores huían de la justicia con una cartera de bitcoins valorada en más de catorce millones de dólares[3].

No obstante, nuestro análisis no pretende llegar, por el momento, a aspectos de esta macro-delincuencia organizada siendo que el objeto del presente artículo será una somera aproximación a la posibilidad de investigar transacciones con monedas virtuales (centrándonos, por el momento, en *bitcoin*) con soporte en la tecnología *blockchain*.

Sintéticamente, ***blockchain* (cadena de bloques) es la base de datos propia del sistema *bitcoin* (entre otros muchos usos) en la que se anota cada una de las operaciones que se realiza con dicha criptomoneda.** *Blockchain* es un sistema de registros contables distribuido entre varios usuarios de una red que organiza y registra la información que genera en bloques cuyo contenido, por aplicación de técnicas criptográficas, deviene, en su integridad, **inalterable y perfectamente identificable.**

Sin entrar, en este momento, en las ventajas e inconvenientes de este tipo de tecnología, en la práctica, una operación realizada en el sistema, una vez comprobada en línea por los usuarios de la cadena con capacidad de verificación (mineros) se incorpora a la cadena de bloques,

---

2 .- https://www.adslzone.net/2019/03/27/dream-market-dark-web-cierre/.

3 .- https://www.adslzone.net/2019/04/24/wall-street-market-cierre/ .

que no es sino un documento electrónico que se encuentra registrado en todos los servidores de la red, y, desde este momento, deviene **inmune a su destrucción o alteración** (la cual, en sistemas como el que estamos hablando, que es un sistema abierto y no permisionado, sólo puede tener lugar si un porcentaje determinado de usuarios de la red se pusieran de acuerdo en manipularla, algo prácticamente imposible en la práctica).

Así las cosas, tenemos, que el **pago de un reloj** inteligente adquirido en una conocida plataforma de productos tecnológicos de la web[4] se puede realizar en *bitcoins* siendo que, desde el momento en que dicha adquisición es verificada por los "mineros" de la red[5] la misma se incorpora a la cadena de bloques y al documento electrónico que, en cualquier momento, cualquier usuario de la red se puede descargar.

Tal como hemos anticipado, desde el momento en que la transacción se incorpora a la cadena de bloques la misma resulta inalterable. Y ello se consigue, al margen de otras técnicas, con el **uso de algoritmos de "*hashing*"**[6]. Una vez realizado el pago del bien adquirido "x" (quien se identificará a través de una clave pública y firmará con su clave privada) transfiere determinada cantidad de *bitcoins* a "y" (a quien identificara con su clave pública o, más específicamente, con su clave pública *hasheada*) haciendo referencia en el mensaje de transferencia al "*hash*" de la operación en virtud de la cual "x" tiene capacidad de disponer de *bitcoins* siendo que la operación realizada recibe, inmediatamente, un nuevo "*hash*" que la individualizará en futuras transacciones.

Denunciada dicha **transferencia como fraudulenta, ¿existe alguna posibilidad de que la misma sea investigada?** Hemos anticipado que quien paga en *bitcoin* ha de conocer, al menos, la clave pública del beneficiario de la transacción quien, en el esquema que estamos siguiendo, sería el "vendedor" del reloj inteligente. El producto adquirido ni llega ni, en este caso, el vendedor tuvo intención de enviarlo nunca incurriendo, presuntamente, en

---

4 .- A modo ejemplificativo, https://www.gearbest.com/ , aunque hay muchas otras que admiten este tipo de pagos (https://academy.bit2me.com/que-puedes-comprar-bitcoin/)

5 .- La actividad de "minar" no es tan sencilla como, en principio, podría parecer porque para conseguir registrar una operación en la cadena de bloques se exige potente capacidad de computación y la resolución de un complejo problema matemático por medio de un algoritmo que sea capaz de encadenar el nuevo bloque creado con los anteriores.

6 .- La función hash es un algoritmo matemático que, aplicado sobre un archivo o item digital cualquiera, da como resultado una determinada secuencia de caracteres. Dicha función tiene la particularidad de que, aplicada sobre un MISMO archivo o item la secuencia de caracteres resultantes es idéntica y basta con la alteración de un solo bit del archivo en cuestión para que el resultado sea completamente diferente.

la comisión de un delito de estafa. ¿Es posible conocer quién está detrás del delito cometido? Lógicamente hemos partido de considerar que la compra del reloj se lleva a cabo en un "sitio" de relativa confianza pero, ¿qué ocurre si el pacto de compra-venta tiene lugar entre particulares?

Más allá del rastro que la operación fraudulenta puede dejar en las redes (imaginemos, por poner un ejemplo, que el acuerdo se haya alcanzado en un foro de discusión o en una aplicación de mensajería instantánea en los que, hipotéticamente, se pueda rastrear el origen de la comunicación) vamos a centrarnos en la posibilidad de investigar esa operación en fuentes abiertas a través de los datos que la red *blockchain* deja.

Y es que **existe una dirección web (https://www.blockchain.com/) que ofrece al investigador un "explorador" de todas las operaciones que se han realizado a través del sistema *blockchain* desde el que podríamos denominar "bloque génesis".**

Accediendo al explorador[7] (a través de la opción Datos > Explorador) se obtiene un listado de todos los bloques registrados en *blockchain*, ordenados cronológicamente. Siquiera sin acceder al "*hash*" que se ha asignado a la operación registrada ya puede individualizarse la hora y el minero a quien se debe el registro de la operación.

Accediendo a los datos del bloque, pulsando sobre el *hash* del bloque generado, nos encontramos con todos los datos contenidos en el bloque: transacciones contenidas en el bloque, cantidad de *bitcoins* de salida, comisiones vinculadas a las transferencias realizadas, *hash* del bloque generado, *hash* del bloque anterior y actas de todas las operaciones contenidas en el bloque.

En cada una de las actas contenidas en el bloque y reflejadas en el registro mencionado nos encontramos, en la parte superior izquierda, con el identificador de la operación, asimismo *hasheado* (e3dfafd6615b66eb9598912391172d55577e7bafb31ca61066e09eba********** donde los "*" pueden ser letras mayúsculas, letras minúsculas o números) , así como con la dirección de *bitcoin* (1NVvVUK7uFG1PLt7sbucJ7tMLM********, donde los "*" pueden ser letras mayúsculas, letras minúsculas o números) que ordena la transacción, en la parte izquierda, bajo el

7 .- Un sencillo copy-paste de la dirección pública a la que se ha transferido el BTC es suficiente para que, a través de este explorador, pueda obtenerse el historial de transacciones de dicha direccion pública.

identificador de la operación, y la dirección de *bitcoin* que la recibe (con el mismo formato), en la parte derecha, así como la cantidad transferida. Incluso resulta posible acceder a todos los datos vinculados a las operaciones realizadas por quien quiera que haya solicitado cualquiera de dichas cuentas.

Obtener una dirección bitcoin es muy sencillo. Simplemente es necesario descargar un monedero (*wallet*) de *bitcoin* y podrás tener tantas cuentas como desees.

Ahora bien, contando con ese dato, **¿es posible determinar quién está detrás de dicha cuenta a la que tan fácilmente puede accederse a través de https://www.blockchain.com/?**

En redes abiertas no permisionados (como es aquella que sirve de soporte a *bitcoin*) **no existe autoridad central alguna a la que dirigirse para que le sea facilitada al investigador la información requerida.** El libro-registro en que la cadena de bloques consiste puede estar en poder de cualquiera que acceda al sistema y, más en concreto, necesariamente, lo está de cuantos nodos operan la red y asumen la función de verificar las operaciones practicadas.

Dirigirse a cualquiera de esos nodos en base a lo dispuesto en el art. 588 ter e)[8], por poner un ejemplo, y la obligación de estos de responder conforme a lo allí establecido presenta tales problemas de interpretación que darían pie a varios artículos completos de la extensión del presente (más allá de los problemas de jurisdicción que pueden generarse como consecuencia de la ubicación de los distintos nodos en Estados fuera de nuestras fronteras, incluso más allá de las de la Unión Europea) con lo que ha de buscarse una alternativa.

La misma puede hallarse en dos momentos:

1.- El primero de ellos hay que buscarlo en el concepto de *wallet* antes mencionado. Los ***wallets* son monederos donde se almacenan las criptomonedas.** En nuestro caso, monederos donde se almacenan *bitcoins*.

Si bien existen *wallets* "fríos", que son aquellos que

8 .- Art .588 ter e) LECRIM: "*Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones*"

no se encuentran conectados a la red, **lo normal es que el usuario acceda a su *wallet* "*online*" mediante la conexión a una página web o instalando un software en el ordenador o en el smartphone.**

A modo de ejemplo, entre las primeras, estaría bitGo (https://www.bitgo.com/info/solutions#wallet) o la propia de Blockchain y entre las segundas estarían, por ejemplo, Electrum (https://electrum.org/#home) o MyCellium.

2.- **El segundo de los pasos sería encontrar el canal oficial donde el titular del *wallet* haya cambiado sus criptomonedas (sus *bitcoin*) por dinero fiduciario. Estamos hablando de los *exchange*.**

Un *exchange* es una plataforma donde se puede intercambiar una criptomoneda por otras e, incluso, por dinero fiduciario.

Un ejemplo de *exchange*, quizá la más conocida y segura, es Coinbase (https://www.coinbase.com/) empresa norteamericana que, además de servicio de *wallet*, presta servicios de intercambio de múltiples criptomonedas así como de criptomonedas y moneda fiduciaria[9].

Pues bien, tomando como referencia la **nueva Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo**, que considera como personas obligadas por su contenido a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias (*exchanges*) y a los proveedores de servicios de custodia de monederos electrónicos (*wallets*) **se puede descartar, una vez implementada en los Estados miembros, la existencia de cuentas de *bitcoin* anónimas (art. 10)** ya que, entre otras, se impone a estas entidades una serie de diligentes obligaciones con relación a sus clientes (art. 13) resultando imperativo para estas entidades la adopción de una serie de medidas (declaraciones, entre otras) destinadas a colaborar en la lucha contra el blanqueo de capitales o la financiación del terrorismo.

Como defiende Fabio Pascua Mateo en "Criptomonedas"[10] la directiva, aún consciente de que la consideración de dichas entidades como obligados no resolverá completamente

9 .- Con participación de entidades bancarias tan poderosas como BBVA: https://www.bbva.com/es/bbva-ventures-invierte-en-coinbase-la-plataforma-lider-de-bitcoin/

10 .- Criptoderecho: La regulación de Blockchain, Director: Pablo García Mexía, Ed. Wolters Kluwer, 2018, páginas 390 y siguientes.

el tema del anonimato en que, en ocasiones, se mueve el usuario de la red en el entorno de *bitcoin* (imaginemos transacciones en la "*dark web*" a través de navegadores como Tor) se centra "*en regular el eslabón más sencillo de la cadena*" siendo ésta, actualmente, la forma más adecuada y accesible para la averiguación de grandes operaciones fraudulentas que, en el entorno *bitcoin*, pueden llegar a perpetrarse.

No obstante, no debemos llevarnos a engaño. **La investigación de este tipo de ilícitos seguirá resultando muy difícil e, incluso, imposible en algunos casos si tenemos en cuenta que la mayor parte de los *exchange* tienen su sede no sólo fuera de territorio español sino, incluso, fuera del ámbito de la Unión Europea** con lo que, más allá de tener que recurrir, necesariamente, a instrumentos de cooperación judicial y/o policial la mencionada Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo no les resultará, siquiera, de aplicación.