ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

34/2021 septiembre de 2021

*David Ramírez Morán*

**Dinero digital**


# Dinero digital

## Resumen:

El dinero digital es una herramienta imprescindible para el mundo actual en el que la mayor parte de las transacciones se llevan a cabo mediante vínculos de confianza entre las partes involucradas y/o un posible tercero que dé fiabilidad a la transacción. Son varios los modelos que han ido surgiendo bajo esta aproximación y en las criptomonedas basadas en tecnologías de confianza distribuida existe preocupación por los usos ilícitos que se pueden hacer gracias a las características de anonimato que pueden tener las transacciones. Este anonimato podría fomentar la utilización de estos medios para financiar y respaldar actividades criminales, aunque, de acuerdo con varios estudios, mientras la delincuencia sí está haciendo uso de estas herramientas, no ocurre lo mismo en los grupos terroristas.

## Palabras clave:

Divisa digital, criptodivisa, terrorismo, delincuencia, moneda digital.

# *Digital money*

*Abstract:*

*Digital money is a requirement for the world in which we live currently, where most transactions are carried out by trust links between stakeholder and/or a maybe third actor that provides trustfulness to the transaction. Several models have appeared under this approach, and it is in cryptocurrencies based on ledger technologies where alerts have emerged given the illicit uses available thanks to the anonymity the transactions may have. Anonymity might foster the use of these tools to fundraise and support criminal activities although, according to different studies, while crime is making use of these tools, this is not the case for terrorist groups.*

*Keywords:*

*Digital currency, cryptocurrency, terrorism, criminality, digital coin.*

## Introducción

El dinero digital lleva bastantes años recibiendo una creciente atención tanto por los sectores especializados como, cada vez más, por el público general. Son varios los modelos que han dado lugar a esta evolución y este es el motivo por el que se ha utilizado el término de dinero digital en este documento.

Dentro de la denominación de dinero digital, y entendiendo este como la posibilidad de hacer operaciones monetarias sin utilizar una moneda tangible, es necesario incluir una tecnología que inicialmente no tenía que ver con el mundo digital, pero en la actualidad depende casi en su totalidad de él. Se trata de las tarjetas de crédito y débito que, en la actualidad, implementan a todos los efectos una digitalización de la moneda tangible, porque los pagos realizados con ellas se basan en una relación de confianza entre las tres partes involucradas, comprador, vendedor y banco emisor. Las transacciones realizadas con estos medios quedan registradas en los sistemas de procesado de las transacciones posibilitando el análisis forense y la identificación de las operaciones y los individuos involucrados.

Antes de la llegada de la primera criptomoneda disponible públicamente, bitcóin, se había detectado el uso alternativo de las monedas o créditos virtuales implementadas en los videojuegos *online* multijugador para la adquisición de los bienes y servicios del juego que permitían una más rápida evolución o poder alcanzar algunos objetivos. Ciertos usuarios se dedicaban a atesorar estas monedas, o créditos, y negociaban a través de las herramientas de comunicación de los propios juegos o a través de plataformas externas la venta de paquetes de estos créditos o de objetos adquiridos con ellos. Las monedas virtuales del entorno de juego se convertían así en activos digitales con una cotización en moneda tangible.

La llegada de bitcóin[1] en 2009 abrió el camino de las criptomonedas y despertó el interés por cuestiones que hoy en día siguen siendo de plena actualidad como la anonimidad de las transacciones, la falta de respaldo de la moneda… Durante los años siguientes fueron surgiendo nuevas monedas basadas en la tecnología de cadenas de bloques para recoger las transacciones. Las nuevas opciones proporcionaban características como mayores medidas de anonimización de las transacciones, otros algoritmos para evitar la

[1] Nakamoto, S. Bitcóin: un sistema de dinero en efectivo electrónico *peer-to-peer*. *Bitcoin.org*. Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

concentración de la capacidad de inclusión de bloques en la cadena o democratizar el minado. Surgieron también nuevos modelos de uso de las cadenas de bloques con plataformas y monedas como ethereum y ether que permiten establecer contratos inteligentes, que son aplicaciones que se cargan en la propia cadena de bloques y se ejecutan de forma totalmente automatizada.

En 2017, se produjo el lanzamiento simultáneo de multitud de ICO. Una Initial Coin Offer (ICO) es el equivalente de la salida al mercado de una empresa donde las acciones se materializan en forma de criptomoneda o *token*, cuyo valor se regirá por la ley de la oferta y la demanda entre los que quieren deshacerse de los *tókenes* y los que los quieren adquirir para formar parte de los inversores de la compañía. En los mercados regulados, ante una oferta pública de venta, lo que tradicionalmente se conoce como salida al mercado, la empresa tiene que cumplir una serie de requisitos que aseguren la transparencia y protección del inversor que vienen impuestos por unos organismos y autoridades que someten la operación a la legalidad vigente. En una ICO toda la responsabilidad se deposita en el emisor de la criptomoneda. No existe ninguna autoridad que analice la operación y su sometimiento a la legalidad vigente. De hecho, no queda clara la legislación que resulta de aplicación. En la práctica, se han dado casos en los que un individuo ha lanzado una ICO que posteriormente ha resultado ser un fraude y se le ha aplicado la legislación nacional para someterle a la acción de la justicia.

Al principio resultaba relativamente sencillo acceder al mundo de las criptomonedas mediante la instalación en el ordenador privado de los programas que incorporan bloques a la cadena de bloques a cambio de una recompensa en forma de cierta cantidad de la propia criptomoneda. Esta operación se denomina «minado» por la similitud con el trabajo de extracción de materias primas. El creciente interés por conseguir criptomonedas con el minado fue expulsando a estos usuarios, pues su capacidad de cálculo quedaba muy por detrás de la de los nuevos actores, que utilizaban *hardware* más específico como tarjetas gráficas o circuitos integrados diseñados específicamente para el minado. Proporcionan un mayor retorno porque realizan las operaciones más rápido, encontrando los resultados correctos con mayor probabilidad, y lo hacen de manera más eficiente en términos energéticos. Con los rápidos aumentos de cotización de algunas criptomonedas debido a los nuevos mineros, la opción del minado estaba totalmente fuera del alcance del usuario normal.

Surgieron las casas de intercambio que permitían adquirir o vender criptomonedas como activos negociables, desligando al cliente de las tecnologías que les dan soporte. Las casas de intercambio constituyen el punto de encuentro entre el mundo financiero tangible y el mundo financiero virtual, pues permiten adquirir activos digitales a cambio de dinero tangible y vender activos digitales a cambio de su contravalor en dinero tangible. Sin embargo, la relación del poseedor de criptomonedas con la infraestructura descentralizada y distribuida requería de nuevo depositar la confianza, especialmente en lo que respecta a la anonimidad, en la plataforma de la casa de intercambio. En la actualidad existen incluso cajeros automáticos en los que es posible adquirir criptomonedas pagando con tarjeta bancaria, aunque, al menos en el caso de España, no son anónimos y requieren proporcionar datos de identificación.

Nuevamente, en un mundo abierto donde se valora la anonimidad de las criptomonedas y las ventajas que proporcionan, se están desarrollando varias alternativas de lo que se denomina DeFi (*decentralized finance*)[2], con las que se persigue devolver al usuario normal de criptomonedas la posibilidad de poder operar sin tener que depositar la confianza en un tercero. Se trata de aplicaciones basadas en el uso de contratos inteligentes que se ejecutan automáticamente por la infraestructura de las monedas digitales, la red distribuida de nodos que gestiona las transacciones. Así se han creado herramientas para la gestión automatizada de préstamos, casas de intercambio descentralizadas, herramientas derivadas que permiten especular con los cambios de cotización de las monedas o bienes en forma de tókenes digitales, NFT, que permiten la venta de activos digitales como arte u otros intangibles.

Los Estados no son ajenos a la evolución de las monedas digitales y están identificando las ventajas que proporcionan con respecto a las monedas tradicionales. Están evaluando la creación de monedas digitales respaldadas por su propia divisa o con recursos propios, con las que establecer un entorno fiable y regulado para que los ciudadanos puedan operar con ellas con total seguridad. Las CBDC (Central Bank Digital Currency) se encuentran en las agendas de numerosos bancos centrales incluyendo el Banco Central Europeo[3], el PBoC (People's Bank of China). También están recurriendo

[2] The Complete Beginner's Guide to Decentralized Finance (DeFi). Disponible en: https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi
[3] A digital euro. *ECB*. Disponible en: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html

a ellas con otros fines como aprovechar la naturaleza descentralizada para establecer vías de negociación que eviten las sanciones impuestas internacionalmente.

En 2019, se anunciaba la intención de Facebook, como principal promotor, y en asociación con otras grandes empresas del sector financiero, de crear una nueva criptomoneda, libra[4], dirigida a facilitar las transacciones financieras de los usuarios de su aplicación. Tal y como está diseñada, plantea un sistema económico paralelo al tradicional para el que todavía no se ha creado la legislación de aplicación ni los mecanismos de encaje en el sistema económico actual.

No hay que olvidar, por último, plataformas como Apple pay o Paypal donde estas plataformas ejercen una labor de intermediario entre el usuario y el banco del que es cliente a través de la tarjeta de pago o la cuenta corriente del usuario. El uso de estas herramientas persigue proteger la información del usuario proporcionando un mecanismo que permite que la información específica de la cuenta o tarjeta con la que se hace una transacción no sea conocida por la parte contraria. Reduce así riesgos tradicionales como el robo del número o el clonado de la tarjeta y protege la privacidad del pagador al ocultar la empresa que gestiona sus finanzas.

## Características de las criptomonedas

Las criptomonedas presentan varias características que las diferencian de las monedas tangibles tradicionales y que constituyen ventajas con respecto a estas últimas en función de los casos de uso o aplicaciones para las que se desean usar.

### *Anonimidad*

La anonimidad que presentan las criptomonedas se fundamenta en la dificultad de identificación del propietario de una cibermoneda, o un saldo de ellas, únicamente a través de un número o secuencia de valores que identifica al usuario individual. La anonimidad de las transacciones en criptomonedas solo es tal mientras no sea posible establecer un vínculo entre el identificador del monedero del usuario y la identidad real del usuario.

[4] Ricou, E. Libra (LIBRA) Coin: Facebook's Cryptocurrency. *Stormgain*. Disponible en: https://stormgain.com/blog/libra-coin-facebooks-cryptocurrency

Criptomonedas como monero aportan un grado adicional de anonimidad porque, a diferencia de otras como bitcóin, se generan nuevos identificadores desechables para el destinatario de cada transacción y solo este puede determinar el origen. Para ofuscar el origen de la transacción incluye el mecanismo denominado de anillo que dificulta identificar el verdadero ordenante de una transacción al hacer que la firma la realice un individuo de entre varios con el mismo balance. También el importe queda oculto mediante el uso de Ring Confidential Transaction de forma que solo los extremos de la transacción conocerán el importe, aunque la transacción aparezca en la cadena.

***Minado***

El minado es la denominación que se aplica a las operaciones informáticas que se utilizan en varias criptomonedas para la incorporación de las transacciones a la cadena de bloques. La seguridad de la cadena de bloques se deposita en la existencia de una prueba que valide la información que intenta incorporar un actor a la cadena de bloques.

La prueba de trabajo es el mecanismo utilizado en las criptomonedas para asegurar la fiabilidad de las transacciones y eliminar la posibilidad de que bloques anteriores de la cadena sean modificados posteriormente.

Uno de los principales factores que afectan a la rentabilidad del minado es el precio de la energía. Ejecutar los algoritmos que permiten encontrar el número que da lugar a un bloque validado requiere de energía eléctrica en cantidades cada vez crecientes. Este es el motivo por el que, en 2019, se estimó que un 65 % de la capacidad de minado de criptomonedas se encontraba en China[5]. Esta concentración de la capacidad de minado supone también un problema para la fiabilidad de las monedas pues el mecanismo de confianza requiere que ninguna de las partes involucradas en el minado disponga de más del 51 % de la capacidad[6] porque, de lo contrario, podría bloquear la red monopolizando el minado.

[5] Huang, R. The 'Chinese Mining Centralization' Of Bitcoin And Ethereum. *Forbes*. Disponible en: https://www.forbes.com/sites/rogerhuang/2021/12/29/the-chinese-mining-centralization-of-bitcoin-and-ethereum/

[6] Disponible en: https://academy.binance.com/en/articles/what-is-a-51-percent-attack

Recientemente aparecía un artículo en un diario generalista sobre la instalación de dispositivos de minado en granjas turcas[7] como herramienta de lucha contra la inflación.

El algoritmo que rige el minado de bitcóin ha dado lugar a lo que se explicaba previamente de expulsión de facto de los pequeños mineros. La capacidad de minado medida en *hash* por segundo alcanza en la actualidad los *exahash* (10 elevado a 15) por segundo para mantener el ritmo de incorporación de bloques de bitcóin de 10 minutos por bloque. Solo utilizando dispositivos específicos de minado es posible conseguir rentabilidad con el minado para cubrir los costes del dispositivo y, especialmente, de la energía necesaria. Ante este escenario, otras monedas han recurrido a algoritmos diferentes que no permiten alcanzar tanta eficiencia mediante el uso de dispositivos dedicados. De esta forma se fomenta que pequeños mineros puedan optar a conseguir las recompensas asociadas a introducir un bloque y se vuelve a hacer viable utilizar un ordenador normal para hacer el minado. Monero es nuevamente un ejemplo de criptomoneda cuyo algoritmo se adapta a estas características.

Sin embargo, esta virtud también se transforma en riesgo porque el ordenador de cualquier usuario de internet o cualquier servidor puede llevarlo a cabo. Esto ha sido explotado tanto por actores lícitos como por delincuentes para utilizar los ordenadores de usuarios y empresas para minar. De forma lícita informando al usuario de que, por ejemplo, mientras esté navegando en una web su ordenador estará minando criptomoneda en beneficio de su propietario, y de forma ilícita mediante la introducción de algoritmos criptomineros de forma fraudulenta en las páginas web de terceros aprovechando alguna vulnerabilidad o consiguiendo acceso a la capacidad de proceso de un servidor de internet vulnerable y utilizando su potencia de cálculo para el minado. En el caso de España, el *Informe de ciberamenazas y tendencias 13/20* del Centro Criptológico Nacional identificaba también esta amenaza[8].

### *Volatilidad de las monedas digitales y criptomoneda estable*

La volatilidad de las monedas digitales es uno de los principales problemas por los que se cuestiona su utilización cotidiana más allá de las operaciones especulativas. Se han

[7] Los turcos apuestan por las criptomonedas como valor refugio ante la inflación. *Expansión*. Disponible en: https://www.expansion.com/mercados/2021/06/19/60cdd409e5fdea226d8b4599.html
[8] Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

dado episodios de gran volatilidad en las criptomonedas motivados por hechos poco relevantes como puede ser la publicación de un Twitter de Elon Musk o la publicación incorrecta de una página web en la que parecía que una gran empresa iba a empezar a admitir como medio de pago una moneda digital. Con gran volatilidad se refiere a variaciones de precio en plazos inferiores a una semana de más del 20 %. 2019 fue un ejemplo de esta volatilidad al empezar bitcóin el año con una cotización alrededor de 1.000 dólares y terminarlo en torno a los 20.000.

Las monedas estables por el contrario son monedas digitales cuya cotización está respaldada por un activo o conjunto de activos físicos como puede ser una divisa, una bolsa de divisas o unas materias primas. Surgen ante el problema que supone la volatilidad de otras monedas cuyo valor fluctúa únicamente en función de la oferta y la demanda. Esta estabilidad de la cotización permite un uso más seguro en términos financieros y evita comportamientos como el *hodling*[9], término utilizado para describir, en el contexto de las criptomonedas, la actitud de un poseedor de ellas que, ante el rápido incremento de su precio, decide conservarlas para beneficiarse de su revalorización en lugar de gastarlas para adquirir activos.

En el caso de las ICO, el respaldo de la criptomoneda es el propio valor real de la compañía. Su cotización responde por tanto a factores habituales en el mundo de las finanzas de las empresas cotizadas. Entran en juego por tanto variables como las expectativas, la evolución de la compañía y todos aquellos factores externos a la compañía que pueden afectar a su modelo de negocio.

### *Fungibilidad*

La fungibilidad es una propiedad que diferencia las monedas entre las que las unidades que forman parte de la divisa pueden ser identificadas de forma individual de aquellas en las que todas las unidades son indiscernibles unas de otras. Las monedas de naturaleza no fungible permiten identificar individualmente una moneda específica y podrían declararse inválidas ciertas monedas, permitir identificar monedas que han sido utilizadas en ciertas operaciones y, por tanto, identificar autores que pueden haber estado involucrados o guardar relación con delincuentes en función de los fondos que

[9] Esta denominación proviene de la errata de un forero que escribió *hodl* en lugar de *hold* cuando exponía que no se desharía de sus criptodivisas para aprovechar el crecimiento de su cotización.

han recibido y a quién se los han enviado. Esta es una característica que diferencia, por ejemplo, las monedas bitcóin, no fungible, y monero. De hecho, la página web de monero destaca esta característica a la hora de demostrar la mayor privacidad y seguridad que presenta esta moneda frente a bitcóin.

### *Análisis forense*

La cadena de bloques asociada a una criptomoneda contiene todas las transacciones realizadas hasta la fecha con la criptomoneda. La identidad de los usuarios se encuentra protegida por los identificadores numéricos de su monedero, pero, si es posible establecer la relación entre un monedero y una persona, se podrían identificar las transacciones realizadas por esta persona. A partir de estas transacciones se podrían seguir adelante o atrás las transacciones realizadas con el fin de identificar quién hizo llegar fondos a esta persona o a quién ha enviado fondos.

Para dificultar esta operación de análisis, se llevan a cabo operaciones denominadas *mezclados*, de *mix* en inglés, por el que el importe de una transacción se somete a un elevado número de transacciones intermedias adicionales con el fin de dificultar la labor de identificación del originario y el destinatario de una transacción. En la actualidad, con la potencia de cálculo y almacenamiento disponible y con la aplicación de inteligencia artificial es posible investigar estas operaciones de mezcla y extraer información del origen y el destino.

Pero, para que las investigaciones forenses permitan llevar a cabo acciones resulta imprescindible que exista o se encuentre el vínculo entre una identidad física y el código o identificador del monedero bajo el que esa persona opera con criptomonedas.

## Los Estados y el dinero digital

### *¿Moneda o activo?*

A los efectos de los Estados esta diferenciación resulta importante por cuanto difiere la legislación de aplicación para los usuarios de las criptomonedas.

En el caso de ser considerado como un activo, los usuarios operarían con ellos adquiriéndolos o vendiéndolos, pagando los impuestos correspondientes al beneficio obtenido.

En la Unión Europea se está trabajando en la regulación de las casas de intercambio para permitir la fiscalización de las operaciones con criptomonedas. Por tratarse de un activo cuya cotización varía con el tiempo, el usuario de la criptomoneda tendrá una ganancia o pérdida patrimonial debida a la diferencia de cotización desde el momento de adquisición hasta el momento de disposición de la criptomoneda.

Fuera de esta capacidad de fiscalización quedarían por lo tanto todos aquellos actores que no recurran a establecimientos de intercambio para la adquisición o disposición de las criptomonedas.

***Venezuela***

En 2018, anunció el presidente de Venezuela, Nicolás Maduro, la creación del petro[10], una criptomoneda que permitiría al país seguir importando y exportando bienes evitando las sanciones impuestas por las que se bloquearon numerosas cuentas en el extranjero dificultando la exportación de sus principales fuentes de ingresos, el petróleo y el gas. El presidente comunicó que cada elemento de la moneda estaría respaldado por un barril de petróleo.

Poco después, el presidente de Estados Unidos, Donald Trump, emitió una orden ejecutiva por la que se prohibían «todas las transacciones relacionadas con, provisión o financiación u otros en […] cualquier divisa digital, moneda digital u objeto digital que fuera emitido por o en beneficio del Gobierno de Venezuela»[11].

Esta criptomoneda ha sido criticada por su escaso impacto en el mundo de las criptomonedas al no estar disponible en casas de intercambio y tener un modelo de uso prácticamente unidireccional en el que solo ciudadanos extranjeros pueden adquirirla para gastarla en bienes y servicios proporcionados en el país.

***El Salvador***

El 6 de septiembre de 2021, bitcóin pasó a ser moneda de curso legal en El Salvador en una medida muy controvertida que ha despertado un importante rechazo social. Con esta

[10] Disponible en: https://petro.gob.ve/es/
[11] Disponible en: https://www.cnbc.com/2018/03/19/trump-issues-action-blocking-us-citizens-from-trading-or-financing-venezuela-cryptocurrency.html

medida tanto los ciudadanos como las empresas tienen obligación de aceptar pagos y cobros con esta moneda.

El rechazo ha venido motivado principalmente por la concepción existente de que las criptomonedas, por sus características de anonimidad, propician los delitos y la corrupción.

Esta medida requiere de la población la incorporación de tecnologías digitales en su día a día, porque solo aquellos que cuenten con la aplicación instalada en su móvil podrán acceder sin comisiones a la criptodivisa.

Se trata de una medida muy controvertida porque deposita el futuro económico de un país en la evolución de una moneda fiduciaria sin ningún tipo de respaldo más allá de la confianza de sus usuarios.

Es interesante evaluar los efectos que tiene introducir el bitcóin en una economía dolarizada como la de El Salvador. Se trata de una economía dolarizada y que, por tanto, ostenta muy poca capacidad para controlar la economía nacional con medidas como el control del cambio de su propia moneda. Solo puede llevar a cabo acciones macroeconómicas por la vía del control de los tipos de interés. La introducción del bitcóin tampoco cambia esta situación pues la cotización de la moneda digital está denominada también en dólares y viene fijada por factores externos. Por lo tanto, el interés de introducir el bitcóin en el país responde a las otras ventajas que reporta como son la reducción de las comisiones por las transferencias de remesas con respecto a los sistemas financieros tradicionales y la reducción de los plazos para completar estas operaciones, aspectos ambos muy relevantes si se tiene en cuenta que «las remesas representan más de 24 % del Producto Interno Bruto»[12] de acuerdo con datos del Banco Mundial.

El uso del bitcóin en el día a día a través del monedero electrónico no supondría ningún problema en el caso de que el país fuera autosuficiente porque, independientemente de su valor fuera de las fronteras, las transacciones puertas adentro no se verían afectadas por tipos de cambio. De esta forma se reducirían las necesidades de divisas, en concreto de dólares que actualmente son necesarios para el funcionamiento de la economía del país. Sin embargo, la realidad no es esta y el país debe realizar tanto importaciones

[12] Disponible en: https://www.criptonoticias.com/comunidad/adopcion/dice-gente-asi-estan-cajeros-bitcoin-chivo-salvador/

como exportaciones que, por lo general, se pagan en dólares. Por lo tanto, los precios de los productos importados sí afectarán al poder de compra de un ciudadano que utilice la criptomoneda para la compra de un producto cuyo precio se haya ajustado a los costes en dólares de sus materias primas.

Mediante la aplicación desarrollada para gestionar el monedero virtual de los usuarios, denominada Chivo, es posible realizar operaciones de compraventa e intercambio de moneda entre la criptomoneda y el dólar sin comisiones. Esta operación está únicamente sujeta a las fluctuaciones de cotización entre ambas divisas por lo que el riesgo de cambio se deposita en todos los ciudadanos.

Para fomentar la introducción de la moneda digital, el Gobierno proporcionará a cada ciudadano que instale el monedero electrónico Chivo un importe de 30 dólares en bitcóin. Se trata de monederos asociados a personas físicas, lo que permitiría un rápido análisis de las transacciones realizadas entre los ciudadanos del país. Este análisis podría facilitar la identificación del fraude fiscal en aquellas operaciones realizadas en criptodivisas. Por lo tanto, de generalizarse el uso de la moneda electrónica frente a la divisa americana en forma de efectivo, podría dar lugar a la reducción de los delitos económicos, la evasión fiscal y la corrupción. El análisis forense de la cadena de bloques permitiría identificar los ingresos y gastos de cada ciudadano e identificar fraudes.

Nayib Bukele, el presidente del país, también adelantó los planes de dedicar energía geotérmica al minado de criptomonedas. De esta forma se persigue intentar localizar en territorio salvadoreño la capacidad de minado que ha salido de China tras la prohibición de minado en ese territorio y proporciona una réplica a las afirmaciones sobre la enorme cantidad de energía que requiere el minado.

***China***

Uno de los países en los que más se han tratado las cuestiones relativas a las criptomonedas es China. Son varios los factores que lo han motivado empezando por la posibilidad de disponer de dinero no controlado por las autoridades.

En 2017, ante los evidentes riesgos que suponían las ICO, las declaraba fuentes de financiación ilícitas y prohibía la negociación con ICO en su territorio[13]. Esta decisión tuvo su rápida respuesta con una caída importante de las cotizaciones de las principales criptomonedas.

El precio de las energías en ciertas áreas del territorio chino dio lugar a una explosión en la implantación de capacidad de minado de criptomonedas, especialmente bitcóin. El minado reporta directamente criptomonedas al propietario del equipo que consigue encontrar la solución algorítmica para incluir un nuevo bloque en la cadena.

La penúltima medida tomada por el país es la prohibición del minado de criptomonedas en su territorio. La huella energética del minado es importante y eran muchas las infraestructuras de minado que se habían localizado en el país para aprovechar los bajos costes de la energía, principalmente hidroeléctrica, en algunas regiones del país.

El 24 de septiembre de 2021, el PBoC ha declarado ilegal toda actividad relacionada con las monedas virtuales «no respaldadas por autoridades monetarias, que utilicen la criptografía, con cuentas distribuidas o tecnologías similares y que existen de forma digital», tanto en su territorio, como llevada a cabo fuera de sus fronteras para prestar servicios a residentes en China[14].

### *Yuan digital*

Desde 2014, China ha estado trabajando en la creación del yuan digital, una moneda digital cuya cotización se corresponde directamente con el yuan tradicional. Por cada yuan digital distribuido por los bancos, estos deberán depositar la misma cantidad a modo de reserva en el PBOC[15]. De esta forma, no existe volatilidad en la cotización de la moneda digital. Sin embargo, la dualidad de monedas permite prácticas económicas como intervenciones de política monetaria sobre determinadas regiones, clases u otros grupos, e incluso podría imponer tasas de interés negativas para el efectivo electrónico con objeto de incentivar el consumo.

[13] China bans initial coin offerings calling them 'illegal fundraising'. *BBC*. Disponible en: https://www.bbc.com/news/business-41157249
[14] Notice on further prevention and disposal of the risk of speculation in virtual currency trading. Disponible en: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4348521/index.html (en chino).
[15] John, A. Explainer: How does China's digital yuan work? *Reuters*. Disponible en: https://www.reuters.com/article/us-china-currency-digital-explainer-idUSKBN27411T

Los ciudadanos utilizan códigos QR que genera el monedero digital para llevar a cabo los pagos y estas transacciones son validadas directamente por el banco, dado que la moneda digital no se basa en una tecnología de confianza distribuida como las cadenas de bloques. Esto permite agilizar las transacciones dado que puede reducirse drásticamente el tiempo necesario para validar la operación.

**Financiación de actividades ilegales**

Las criptomonedas se asocian con frecuencia a las actividades ilegales porque proporcionan un anonimato en las transacciones electrónicas que no es posible conseguir con los sistemas bancarios tradicionales. Es posible intercambiar criptomoneda entre dos individuos no identificados sin necesidad de confiar en terceras partes. Sin embargo, este anonimato desaparece cuando hay que convertir la moneda virtual en moneda tangible o bienes. Entonces es cuando el tenedor de una criptomoneda debe relacionar el identificador anónimo con una identificación del mundo real.

En la reunión del G20 celebrada en Argentina en 2018, se informaba a «[f]inance ministers and central bankers from the world's 20 largest economies meeting in Buenos Aires will be told on Tuesday that such 'crypto assets' do not threaten financial stability but can serve to launder money or finance terrorism and hurt consumers who buy them»[16], donde quedaba reflejado que la capitalización del mercado de divisas digitales no suponía un riesgo para la estabilidad financiera mundial y, por tanto, para su seguridad, aunque sí existían escenarios donde estas herramientas podían contribuir a fomentar la inseguridad facilitando el lavado de dinero, la financiación del terrorismo y dañar económicamente a aquellos consumidores que las adquirieran.

Recientemente, un antiguo empleado de la CIA ya retirado, relacionado con una empresa dedicada a la inteligencia de criptomonedas, publicaba un documento en el que también llegaba a la conclusión de que en la actualidad las criptomonedas no proporcionan la anonimidad que se requiere para las actividades delictivas y que ya existen mecanismos para poder aplicar inteligencia a las cadenas de bloques e identificar comportamientos sospechosos. Se dispone de capacidad para poder analizar las operaciones más

[16] Canepa, F. G20 leaders to hold fire on cryptocurrencies amid discord: sources. *Reuters*. Disponible en: https://uk.reuters.com/article/us-g20-argentina-bitcoin/g20-leaders-to-hold-fire-on-cryptocurrencies-amid-discord-sources-idUKKBN1GV2QR

complejas de mezcla aplicando técnicas de inteligencia artificial[17]. La gráfica de la figura 1 muestra cómo el porcentaje de actividad ilegal cayó abruptamente con el cierre de la tienda de productos ilegales como drogas y armas, Silk Road; y cómo, desde entonces, de acuerdo a los criterios de la compañía que elabora el estudio, se sitúa por debajo del 1 % de la actividad registrada en las criptomonedas.

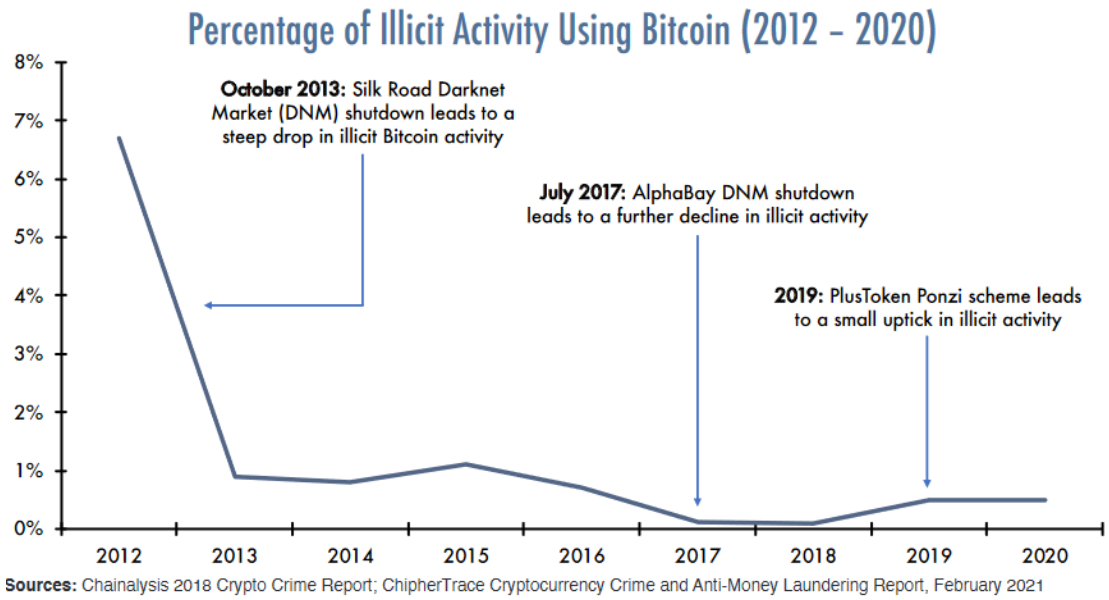
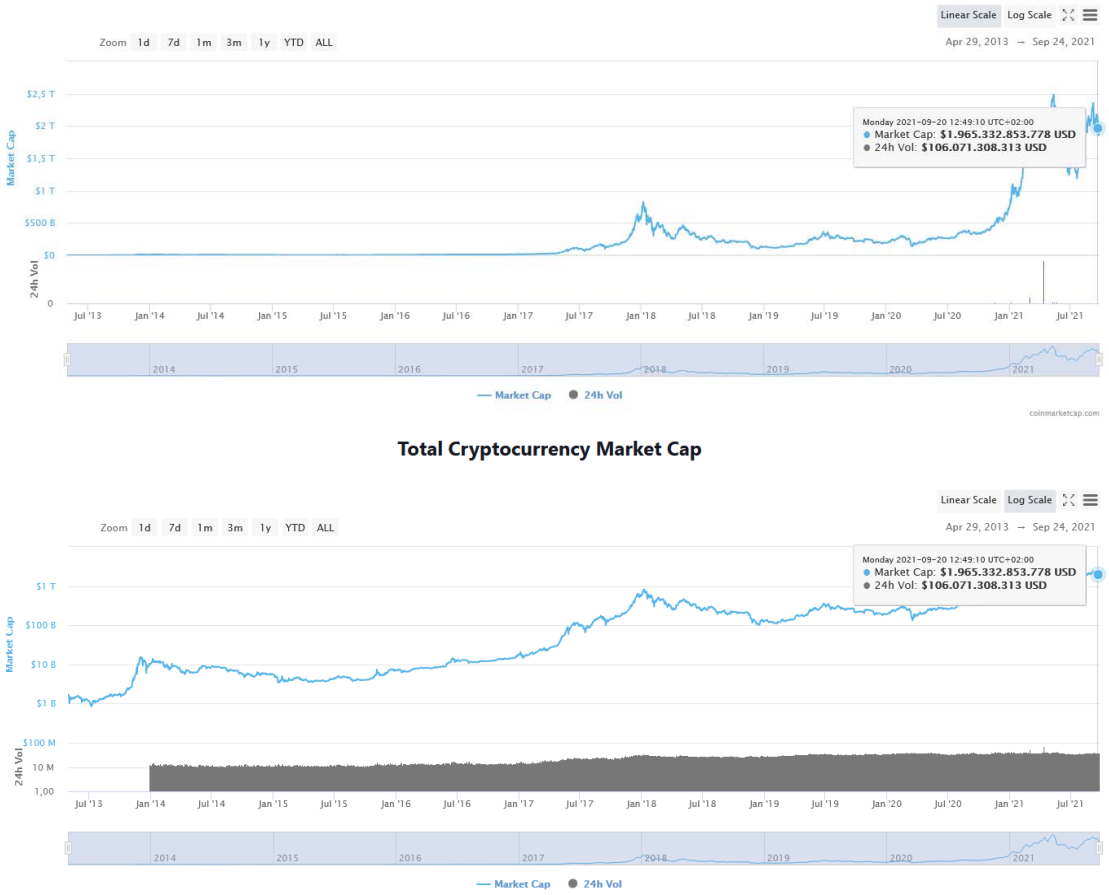



Figura 1. Evolución de la actividad ilícita usando bitcóin. Fuente: Morell

A su vez, en la figura 2 se puede observar que la capitalización total de todas las criptodivisas no llega a los dos billones de dólares que, pese a suponer un importe mayor al PIB de España, a efectos globales no constituye un importe suficiente como para afectar a la estabilidad financiera global.

[17] Morell, M. *et al.* An Analysis of Bitcoin's Use in Illicit Finance. *Crypto for Innovation*. Disponible en: https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf




**Total Cryptocurrency Market Cap**

Figura 2. Evolución de la capitalización de las criptomonedas. Disponible en: https://coinmarketcap.com/charts/

## Sanciones

Las monedas distribuidas suponen para los Estados una alternativa a los sistemas financieros internacionales. Aquellos Estados objeto de sanciones pueden ver sus cuentas en el extranjero bloqueadas de forma que no pueden realizar operaciones como la importación o la exportación de productos ni acceder a los fondos depositados en esas cuentas. En las monedas distribuidas no existe ninguna autoridad que pueda llevar a cabo este bloqueo por lo que los Estados sancionados podrían seguir llevando a cabo operaciones con aquellos actores que estén dispuestos a utilizar ese modo de pago.

**Terrorismo**

Como se indicaba anteriormente, existe preocupación internacional por los usos que los terroristas pueden hacer de las criptomonedas.

La Unión Europea trató este tema en un estudio realizado en mayo de 2018[18]. Se concluía también que el uso por parte de grupos terroristas de criptomonedas para llevar a cabo sus actividades era testimonial y que hoy en día no constituía un riesgo importante.

Rand Corporation publicó un extenso estudio[19] en esta línea que trataba este problema con un análisis para varios grupos terroristas con objeto de poder exponer las diferentes situaciones en las que podían hacer uso de las criptomonedas según su estructura y funcionamiento particular.

En el documento se analizan las cinco actividades identificadas como de mayor interés para las organizaciones terroristas: financiación, tráfico ilegal de armas y drogas, envío y recepción de fondos, financiación de los ataques y financiación operacional.

Para poder llevarlas a cabo identificaban las características necesarias para que las cripotomonedas fuesen de utilidad para los grupos terroristas: anonimidad, usabilidad, seguridad, aceptación, fiabilidad y volumen; y concluían que en la actualidad ninguna de las principales criptomonedas existentes satisface todos estos criterios simultáneamente. Sin embargo, alertaban de que el continuo avance en la tecnología de las criptomonedas requiere seguir haciendo el seguimiento del mercado para identificar cuándo pudieran darse estas características simultáneamente.

Concluían, en línea con los resultados obtenidos, que la alarma existente en esta línea no constituye en la actualidad un riesgo importante.

[18] Keatinge, T., Carlisle, D., Keen, F. Virtual currencies and terrorist financing: assessing the risks and evaluating responses. *Europarl*. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

[19] Dion-Schwarz, C., Manheim, D., Johnston, P. B. Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats. *RAND*. Disponible en: https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

**Delincuencia**

La delincuencia es el ámbito que actualmente más uso está haciendo de las criptomonedas para beneficiarse del anonimato que proporcionan. El escenario en el que desarrollan sus actividades es muy diferente al del terrorismo y, por tanto, no requieren las mismas características que los grupos terroristas. Las soluciones existentes en la actualidad ya resultan suficientes para cumplir las necesidades de sus operaciones y, de hecho, se están produciendo continuamente.

Las estafas *online* como el timo del CEO, por el que el delincuente se hace pasar por el gerifalte de la organización y encarga a los órganos financieros que realicen transferencias urgentes, el acceso a las cuentas corrientes de los usuarios de bancos o el robo de credenciales están a la orden del día. El fenómeno del *ransomware* por el que el atacante aprovecha una vulnerabilidad de los sistemas, cifra la información y luego solicita un rescate para proporcionar la clave de descifrado también se produce con mucha frecuencia. Todos estos ataques conllevan la necesidad de conseguir que el dinero estafado llegue a las arcas del delincuente y es ahí donde las criptomonedas están siendo utilizadas.

A efectos ilustrativos, se recogen a continuación dos casos significativos en esta línea como es el ya famoso caso de Colonial y cómo se están empezando a tomar medidas para reducir la impunidad con la que es posible utilizar las criptomonedas para el crimen.

**Ataque a Colonial**

El ataque de la infraestructura informática de la empresa americana de distribución de combustible Colonial tuvo unos efectos colaterales que llegaron a afectar incluso a la cotización del petróleo. De hecho, el incidente se consideró una emergencia nacional porque el ataque produjo problemas de suministro de hidrocarburos en gran parte de la costa este de Estados Unidos.

Se trató de un ataque de secuestro de los sistemas, un *ransomware*, por el que se solicitaba una recompensa para recuperar la información y el control de los activos informáticos de la empresa. Este fue el efecto más visible del ataque, aunque no se puede descartar que, además del secuestro, previamente los criminales obtuvieran información confidencial o alterasen el funcionamiento de los sistemas de la empresa.

El pago de esta recompensa se realizó mediante bitcóin a la dirección indicada por los secuestradores. A los pocos días, se recuperó una parte importante de la recompensa porque la clave secreta que protege el monedero electrónico del grupo que había lanzado el ataque se encontraba a disposición de las autoridades estadounidenses y pudieron recuperar parte de los fondos del rescate[20]. El resto de los fondos no se pudo recuperar porque habían sido remitidos a otra de las partes implicadas en la operación, una organización que presta servicios, cede su infraestructura, para llevar a cabo operaciones como la ocurrida.

**Sanciones a casas de intercambio**

Recientemente, se ha producido un hecho relevante cuando desde Estados Unidos se ha sancionado a una casa de intercambio rusa por su contribución al lavado de criptomonedas «por dar soporte material a la amenaza que suponen los autores criminales de *ransomware*». Según la investigación realizada, una parte importante del volumen de criptomonedas que llegaban a la empresa provenían de actividades ilegales como ataques de *ransomware*, estafas, mercados ilegales, etc.[21].

[20] Ducklin, P. How could the FBI recover BTC from Colonial's ransomware payment? *Naked Security*. Disponible en: https://nakedsecurity.sophos.com/2021/06/09/how-could-the-fbi-recover-btc-from-colonials-ransomware-payment/
[21] Lakshmanan, R. US Sanctions Cryptocurrency Exchange SUEX for Aiding Ransomware Gangs. *The Hacker News*. Disponible en: https://thehackernews.com/2021/09/us-sanctions-cryptocurrency-exchange.html

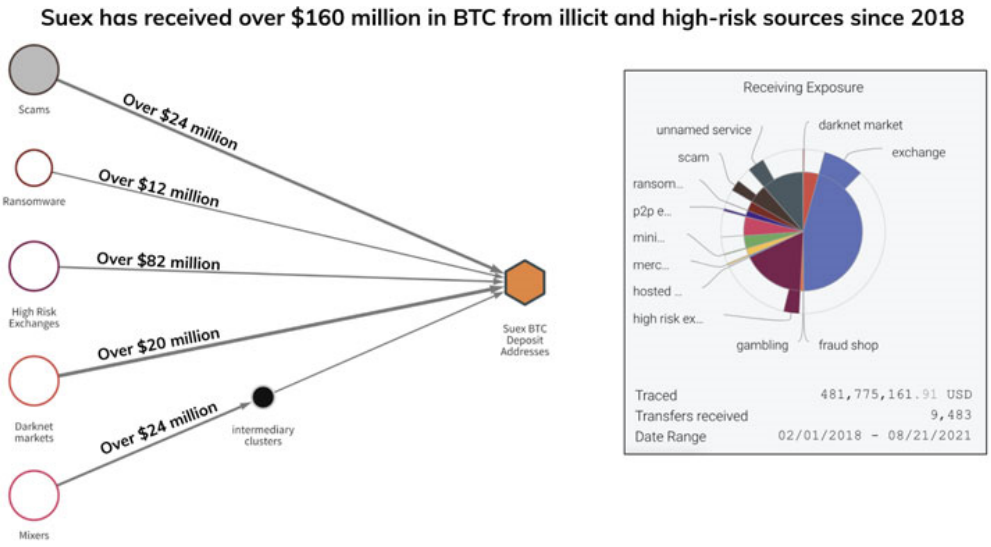



Figura **3**. Desglose de ingresos en SUEX. Disponible en: www.thehackernews.com

## Conclusiones

El dinero digital es una realidad hoy en día y es previsible que, dada la creciente digitalización de las sociedades a nivel global, no haga más que crecer. Los bancos centrales están trabajando para que los ciudadanos puedan aprovechar las ventajas que estas tecnologías aportan en un entorno seguro y confiable.

Pese a la percepción general de que las criptomonedas se utilizan para fines ilícitos, que se ve alimentada por la continua aparición de casos en los que han aparecido como herramientas necesarias para el delito, existe también un creciente interés por parte del sector privado en estas nuevas herramientas financieras.

La principal fuente de riesgos para la seguridad que supone hoy en día las criptomonedas tiene naturaleza eminentemente económica y proviene principalmente de la falta de regulación. Esta regulación, o bien no está completa o bien no resulta de fácil aplicación ante tecnologías distribuidas que carecen de nacionalidad y responsables.

En el caso de los países más desarrollados, donde el uso de medios de pago electrónicos está más generalizado, la implantación de una moneda digital frente a la alternativa tangible apenas supone una diferencia para la gran mayoría de usuarios. En el caso de eliminar la moneda tangible, el impacto sobre la actividad sería poco perceptible, aunque

las actividades ilícitas que hacían uso de pagos mediante efectivo se verán abocadas a modificar sus prácticas.

En sociedades menos desarrolladas, la implantación de monedas digitales supone un doble reto ante la necesidad de generar la confianza necesaria entre la población y conseguir proporcionar los medios tecnológicos, infraestructuras y dispositivos, así como la formación necesaria, para que ningún segmento de la población quede excluido de la revolución digital de los pagos.

La digitalización de los pagos es una herramienta que puede contribuir a la reducción de la corrupción y el fraude por cuanto toda transacción deja un rastro. Sin embargo, esta ventaja a los efectos de la lucha contra el delito se consigue a expensas de la pérdida del anonimato que se consigue con el uso de efectivo y, a más, puede suponer una violación de la intimidad de los ciudadanos. En ámbitos represivos puede constituir una importante herramienta de control de la población y proporcionar a los gobernantes o a las empresas información.

Mientras que en el área de la delincuencia sí están identificadas numerosas actividades que se benefician de las características de las monedas digitales, también es cierto que las capacidades que los Estados están desarrollando para analizar la información está decantando el enfrentamiento hacia el lado de las fuerzas del orden.

Por el contrario, dos son los informes que concluyen que el uso de las criptomonedas para la financiación del terrorismo hoy en día es testimonial porque no proporcionan las características necesarias para que estos grupos las puedan utilizar de forma segura para llevar a cabo sus actividades. Por tanto, la alarma generada alrededor de las criptomonedas a este respecto se puede considerar injustificada en tanto en cuanto la tecnología de las criptomonedas no desarrolle las funcionalidades de las que actualmente carece.

*David Ramírez Morán**
Analista principal del Instituto Español de Estudios Estratégicos