Cuadernos de la Cátedra
CaixaBank de Sostenibilidad
e Impacto Social

Nº 54
Noviembre del 2022

# Ética y criptomonedas

## Hacia un modelo ético y sostenible de monedas digitales

**Javier Pardo Torregrosa**

**Joan Fontrodona**

IESE Business School
University of Navarra

Cátedra CaixaBank
de Sostenibilidad
e Impacto Social

# Ética y criptomonedas

## Hacia un modelo ético y sostenible de monedas digitales

**Javier Pardo Torregrosa**

Asistente de investigación

**Joan Fontrodona**

Profesor de Ética Empresarial y Análisis de Situaciones de Negocio y titular de la Cátedra CaixaBank de Sostenibilidad e Impacto Social

**Edición:** Caja Alta Edición & Comunicación (www.cajaalta.es)
**Diseño:** IESE Business School – www.iese.edu

# ÍNDICE

# 1. INTRODUCCIÓN

En la última década, las criptomonedas han adquirido popularidad en todo el mundo. Han despertado interés entre inversores, empresas y multitud de particulares, que han adquirido este tipo de activos digitales. La pandemia ha acelerado esta tendencia y estos criptoactivos han ganado una presencia cada vez mayor en el sistema financiero, hasta alcanzar a finales del 2021 una capitalización por encima de los tres billones de dólares (Otero y Oliver, 2022). Debido a su importante peso en la economía, su elevada volatilidad y su interrelación con el sistema financiero, los Gobiernos y los bancos centrales han estado observando su evolución y comportamiento con cautela, preocupación y cierto recelo.

Las criptomonedas tienen su origen en un artículo publicado en la plataforma Mtezdow en octubre del 2008 (Nakamoto, 2008), tras el estallido de la crisis financiera, por una persona o un grupo de personas, identificado bajo el pseudónimo *Satoshi Nakamoto* —hoy en día aún se desconoce su verdadera identidad—, en el que se planteaba la creación del bitcóin, una moneda virtual basada en un sistema de pago electrónico de usuario a usuario *(peer-to-peer)*, cuyas transacciones quedaran registradas en una red pública y descentralizada. Mediante el uso de la tecnología criptográfica, las transacciones quedarían registradas de forma segura en una cadena de bloques. Es decir, la propuesta de Nakamoto no requería de intermediarios ni del control de autoridades centrales para solventar la problemática del doble gasto o de la confianza entre las partes (Nakamoto, 2008; Porras y Daugherty, 2021). Así pues, este nuevo activo digital e instrumento de pago, basado en la tecnología criptográfica popularmente conocida como *blockchain* ('cadena de bloques'), pretendía erigirse como alternativa a las monedas fíat respaldadas por los Estados soberanos y establecer un sistema descentralizado, que escapara del control y la intermediación de las autoridades centrales.

**[...] este nuevo activo digital [...] pretendía erigirse como alternativa a las monedas fíat respaldadas por los Estados soberanos y establecer un sistema descentralizado [...].**

Pocos meses después de la publicación del mencionado artículo, el bitcóin empezaba a operar de forma discreta. En los años siguientes fue ganándose la confianza de los usuarios e inversores al garantizar su funcionamiento de forma segura, rápida y eficaz, por lo que el activo digital experimentó una lenta revalorización. En el 2017, su valor inició una acelerada subida originada por la especulación e inauguró una nueva etapa marcada por la volatilidad. Se registraron ascensos pronunciados y bruscas caídas, con oscilaciones del 80% de su valor entre el 2017 y la actualidad. A pesar de la volatilidad que presenta, a lo largo de estos años han ido surgiendo nuevas iniciativas y hoy en día podemos encontrar miles de criptomonedas diferentes (Arnal *et al.*, 2021).

El auge de las criptomonedas ha suscitado un intenso e interesante debate en la esfera política, económica y financiera. Algunos defienden que se trata de un avance hacia la democratización del sistema financiero y esperan que las divisas y finanzas descentralizadas acaben sustituyendo el modelo vigente, que consideran sometido a una excesiva autoridad de los bancos centrales. También defienden que, en los países en vías de desarrollo, los usuarios se verían beneficiados por la posibilidad de ejecutar transacciones de forma rápida y segura, además de evadir el control ejercido por parte de regímenes corruptos. Otros consideran que la tecnología subyacente podría introducir mejoras en los servicios financieros en materia de seguridad, transparencia o programabilidad. En cambio, sus detractores ven las criptomonedas como un gran fraude, dirigido por unos pocos y basado en un modelo de burbuja especulativa que permite, además, la financiación de actividades delictivas. En todo caso, de momento las criptomonedas están lejos de sustituir al sistema monetario y financiero actual, en parte debido a sus limitaciones para ejercer las tres funciones básicas y tradicionales del

dinero: ser unidad de cuenta, depósito de valor y medio de pago. Muy pocos contratos se facturan en criptomonedas, su uso como forma de pago es limitado y su elevada volatilidad impide que se conviertan en un depósito de valor seguro. Las criptomonedas no disponen por ahora de una aceptación genérica y universal, pues no son aceptadas en la inmensa mayoría de las transacciones económicas o financieras (Banco de España, 2022; Conklin y Ceballos, 2022; Otero y Oliver, 2022).

**Las criptomonedas no disponen por ahora de una aceptación genérica y universal [...].**

Al hilo del mencionado debate y teniendo en cuenta que nos encontramos ante una nueva propuesta de modelo monetario y financiero, creemos necesario que la sociedad afronte una reflexión seria, serena y profunda no solo sobre su viabilidad política y económica, sino también sobre aquellas cuestiones relativas a las criptomonedas que afectan al campo de la ética, además de investigar cuál puede ser su impacto social o medioambiental. Este cuaderno explica, en su primer apartado, la naturaleza y el funcionamiento de las criptomonedas y aborda, a continuación, los distintos riesgos éticos, sociales y medioambientales derivados de su utilización. Por último, se ofrecen algunas recomendaciones que pueden servir para utilizar de forma ética y responsable el nuevo modelo de divisas digitales y la tecnología de registro descentralizado que lo sustenta.

# 2. LAS CRIPTOMONEDAS

## 2.1. EL DINERO FÍAT, EL SISTEMA DE PAGOS Y LAS CRIPTOMONEDAS

La creación del dinero se produjo con el advenimiento de las sociedades complejas a finales del tercer milenio antes de Cristo. En las civilizaciones antiguas, algunos bienes o mercancías —como el ganado, las semillas, la sal, el oro, la plata u otros metales— ejercían la función del dinero y podían ser intercambiados en el mercado por otros bienes o servicios. Este tipo de dinero primitivo tenía un valor intrínseco, que se correspondía con el del propio bien. Más tarde, en torno al siglo VII a. C., surgió la moneda de forma simultánea en las civilizaciones de China y Grecia. A lo largo de los siglos, las distintas ciudades, reinos e imperios de Oriente y Occidente fueron acuñando sus propias monedas, principalmente de oro y plata. Su valor era equivalente al del material con el que se habían confeccionado. A partir del siglo XVIII, empezó a emitirse dinero diseñado con otro tipo de materiales más baratos, que estaba respaldado por algún tipo de mercancía o bien subyacente con valor intrínseco, como el oro o la plata. Es decir, el dinero dejó de tener el valor del material que lo componía y se convirtió en una representación del valor del bien o la mercancía subyacente. Este modelo, al que se denominó *patrón oro*, estuvo vigente, con algunas excepciones, hasta 1971, año en el que el por entonces presidente de Estados Unidos, Richard Nixon, acordó que el dólar dejara de ser convertible en oro. A partir de entonces, el valor del dinero se basa en la confianza que genera la autoridad bancaria central de un Estado soberano. Es decir, el sistema se sostiene sobre un acuerdo tácito en el que la sociedad acepta el valor de la divisa, de ahí que se le denomine *dinero fíat* o *fiduciario* (del latín; 'hágase', 'que así sea'). Por tanto, el dinero no deberá estar respaldado por reservas de oro ni de ningún otro bien o mercancía, sino que tiene su fundamento en la confianza generada por la propia autoridad central (Nieto y Hernáez, 2018; Ossa, 1992).

En la actualidad, los bancos centrales, además de emitir el dinero de curso legal, tienen competencias para regular y supervisar el sistema de pagos, el cual admite transacciones en efectivo y pagos electrónicos. Las primeras se efectúan mediante el traspaso de una representación física del dinero de curso legal, es decir, billetes o monedas emitidos por un Estado. El valor del dinero se transfiere sin necesidad de que intervenga la autoridad central, mediante la transmisión de su representación física, de tal manera que quien ostente la posesión de los billetes o las monedas será su propietario. En cambio, en un sistema de pagos electrónicos, la representación del dinero reside en un archivo de datos. Si aplicamos en este segundo caso la lógica de los pagos en efectivo, corremos el riesgo de que los datos del archivo sean copiados y se pueda enviar el mismo dinero a dos o más destinarios a la vez, lo que se conoce como el *problema del doble gasto*. Para superar esta dificultad, el sistema de pagos electrónico contempla la intervención de una autoridad central en la que las partes deben confiar, que ejerce de intermediario. Esta debe registrar la operación y verificar la legitimidad del pago, comprobando que el emisor dispone de los fondos y que estos no se han enviado aún a ningún otro destinatario (Banco de España, 2022; Berentsen y Schar, 2018).

**Al tratarse de un activo digital, no disponen de representación física [...].**

**Si bien el valor de las *stablecoins* se encuentra referenciado al activo que ejerce de respaldo, en el resto de las criptomonedas el valor depende de la confianza de los usuarios.**

Se aborda a continuación la naturaleza de las criptomonedas, denominadas también *monedas digitales*. Al tratarse de un activo digital, no disponen de representación física y solo en algunas ocasiones —es el caso de las conocidas como *stablecoins*, identificadas como *e-money tokens* y *asset-referenced tokens*— se encuentran respaldadas por monedas fíat u otros activos físicos. Si bien el valor de las *stablecoins* se encuentra referenciado al activo que ejerce de respaldo, en el resto de las criptomonedas el valor depende de la confianza de los usuarios. A diferencia del dinero fíat, las monedas digitales

no son emitidas ni se encuentran reguladas por ningún banco central ni por ninguna autoridad que derive de un Estado. La emisión de las monedas se efectúa también de forma descentralizada. Por ejemplo, la emisión de bitcoines se realiza a través del proceso de verificación y registro de las operaciones por parte de los propios usuarios, los cuales pueden obtener nuevos activos como recompensa a la creación e incorporación de nuevos bloques a la cadena. En la mayoría de los casos, las decisiones que atañen a la moneda digital se toman por consenso de los usuarios y no se dispone de una autoridad central (Banco de España, 2022).

Por otro lado, al ser una moneda digital, el activo se almacena en bases de datos digitales y solo se puede transferir a través de transacciones electrónicas. A diferencia del sistema convencional, la verificación del pago se efectúa de forma descentralizada. Es decir, no requiere de una autoridad central a fin de solventar la problemática del doble gasto o asegurar la confianza entre las partes. Son los propios usuarios quienes, incentivados por la obtención de nuevos activos, verifican por consenso la validez de la operación, registrándola de forma encriptada en una cadena de bloques (Banco de España, 2022).

**Son los propios usuarios quienes, incentivados por la obtención de nuevos activos, verifican por consenso la validez de la operación [...].**

Por tanto, las criptomonedas, también denominadas *criptodivisas*, pueden definirse como un activo digital que utiliza la tecnología *blockchain* y que tiene como fin principal desarrollar, aun de forma imperfecta, las tres funciones clásicas de las monedas fiat: servir como medio de pago, como depósito de valor y como unidad de cuenta. No se encuentran reguladas por una autoridad central y su valor depende, por lo general, de la confianza que los usuarios depositan en su activo digital (PwC, 2021). Además de las funciones básicas que comparten con las monedas tradicionales, las criptomonedas pueden ejercer otro tipo funciones distintas a las del dinero, como ser portadoras de derechos en el marco de un contrato inteligente (*smart contract*) o ejercer como activo financiero o de inversión.

## 2.2. FUNCIONAMIENTO DE LAS CRIPTOMONEDAS Y TECNOLOGÍA *BLOCKCHAIN*

En este apartado se explica, a grandes rasgos, la tecnología que está detrás de la mayoría de las criptomonedas y se describe cómo se realizan las transacciones. Con la finalidad de desentrañar la naturaleza, el funcionamiento y las características de las monedas digitales tomaremos como referencia el bitcóin (en especial, el método de validación de transacciones, el uso de la tecnología *blockchain*, la finalidad del activo, la ausencia de respaldo o el régimen de descentralización), pues se trata de la primera criptomoneda en aparecer y su funcionamiento ha sido replicado en gran medida por el resto de las divisas digitales.

**Algunos activos digitales disponen de su propia red *blockchain*, mientras que otros utilizan las plataformas ya creadas por distintos criptoactivos.**

El concepto de bitcóin puede hacer referencia tanto a la plataforma *blockchain* —basada en la tecnología de registro descentralizado— en la que opera la divisa (en la cual se verifican y registran las transacciones) como a la representación de su activo o moneda digital, también denominado en algunas ocasiones *token* ('ficha'). Algunos activos digitales disponen de su propia red *blockchain*, mientras que otros utilizan las plataformas ya creadas por distintos criptoactivos. En este punto, se ha generado cierta confusión en torno al concepto de *token*, puesto que, en algunos estudios, hace referencia a cualquier activo digital (ya sea monetario, de utilidad o de inversión) que opera en una red *blockchain*, mientras que, en otros, se limita a aquellos activos digitales que operan en una plataforma de otro criptoactivo. En este cuaderno, atribuimos la condición de token a cualquier activo digital (monetario, de utilidad o de inversión) que opera en una red de registro descentralizado. (; Berentsen y Schar, 2018; Houben y Snyers, 2018; Otero y Oliver, 2022; PwC, 2021).

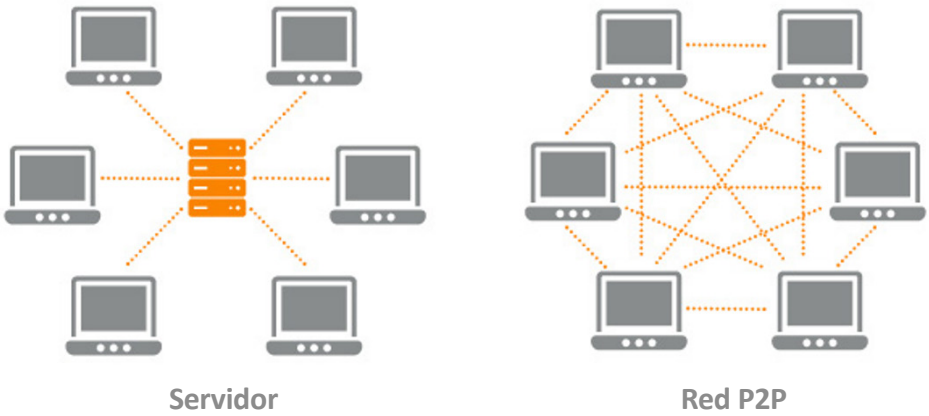
Los usuarios de la red pueden comprar o vender las criptomonedas. Algunas de ellas, además, pueden dividirse en unidades transferibles más pequeñas, como es el caso del bitcóin, que puede fraccionarse en 100 millones de satoshis. Las operaciones se efectúan una vez que han sido validadas y registradas en la base de datos descentralizada de tecnología *blockchain*. El saldo de criptomonedas que posee un usuario de la red queda registrado de forma indirecta en la plataforma al agregar los saldos recibidos y descontar los saldos gastados. Dado que se trata de la representación de una moneda digital, los activos que cada uno posee —además de quedar registrados de forma indirecta en la red— son almacenados en monederos digitales, que en realidad son portales web o programas administrados por intermediarios que custodian las claves privadas con las que los usuarios acceden a la red y efectúan las transacciones (Berentsen y Schar, 2018; Conesa, 2019).

La tecnología *blockchain* que utilizan la mayoría de las criptomonedas se encuentra bajo el paraguas de la denominada *tecnología de registro descentralizado (distributed ledger technology* o DLT), la cual se ha diseñado, a su vez, sobre la base de sistemas tecnológicos ya creados con anterioridad. En concreto, en la construcción de las redes de registro descentralizado se han utilizado las siguientes tecnologías (Otero y Oliver, 2022; Romero, 2018):

**La red se configura como una multitud de conexiones entrelazadas entre los usuarios que almacenan la información de forma descentralizada y a través de los cuales transcurren las comunicaciones.**

- **Las redes *peer-to-peer* (‘de usuario a usuario’, ‘entre iguales’).** A diferencia de un sistema centralizado, las comunicaciones entre los usuarios no necesitan de un servidor central que haga de intermediario. La red se configura como una multitud de conexiones entrelazadas entre los usuarios que almacenan la información de forma descentralizada y a través de los cuales transcurren las comunicaciones. En la siguiente figura podemos observar la diferencia entre una red de comunicaciones centralizada a través de un servidor y una red *peer-to-peer*.

**Figura 1. Diferencia entre una red de comunicaciones centralizada a través de un servidor y una red *peer-to-peer***

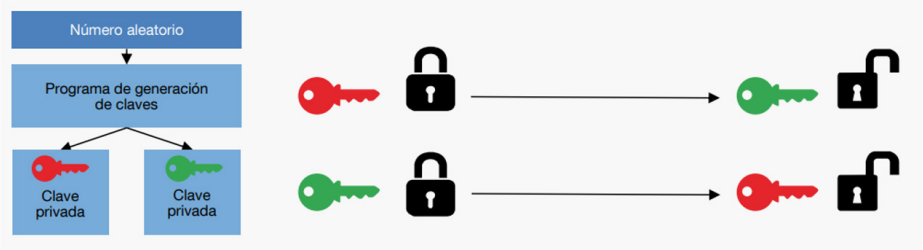



Fuente: Valenzuela (s. f.).

- **La criptografía.** Es un procedimiento que utiliza un algoritmo para encriptar un mensaje, que impide el acceso a todo aquel que no disponga de la clave de cifrado. Se utiliza habitualmente para proteger la confidencialidad del mensaje y también para asegurar la identidad de los usuarios. En la criptografía simétrica, el emisor debe comunicar la clave al receptor, por lo que no queda totalmente resuelto el problema de seguridad, ya que alguien podría interceptar el mensaje

en el que las partes intercambian la clave y, a continuación, descifrar el mensaje encriptado. Desde hace ya algunas décadas, se utiliza en el campo de la informática una versión de criptografía asimétrica o de dos claves relacionadas entre ellas a través de un algoritmo, de modo que una de estas se mantiene en secreto, mientras que la otra es pública para toda la red. Es decir, a través de un algoritmo se obtienen ambas claves, la pública y la privada. Si se usa la clave pública para encriptar, el mensaje solo podrá descifrarse con la privada; y, a la inversa, si se encripta con la privada, solo se podrá descifrar con la pública. De esta manera, se consigue verificar la identidad del usuario y encriptar el mensaje (Conesa, 2019).

**Figura 2. Criptografía asimétrica**




Fuente: Conesa (2019).

- **Los algoritmos consensuales.** Permiten que, ante la ausencia de una autoridad central, varios usuarios de una misma red que desconfían los unos de los otros puedan tomar decisiones mediante mecanismos de consenso.

A continuación, veremos cómo la tecnología de registro descentralizado *blockchain* hace posible el funcionamiento del sistema de pagos con bitcoines o con otras criptomonedas. Este sistema se constituye como una red *peer-to-peer*, en la que los usuarios se interrelacionan en un plano de igualdad sin necesidad de un servidor central. Es decir, estos utilizan multitud de conexiones entrelazadas para comunicarse sin la intermediación de una autoridad central. También utilizan la criptografía asimétrica o de doble clave para asegurar tanto la confidencialidad de las operaciones como la autentificación del emisor de una transacción (Conesa, 2019):

**Mediante la criptografía asimétrica, estos se identifican con la clave pública —que funciona como una especie de número de cuenta bancaria— [...].**

- **Confidencialidad:** puesto que la *blockchain* es una red pública en la que todos los usuarios pueden acceder a la información, es importante mantener el anonimato de aquellos para asegurar la confidencialidad de las operaciones. Mediante la criptografía asimétrica, estos se identifican con la clave pública —que funciona como una especie de número de cuenta bancaria—, sin que sea necesario que revelen su identidad real.

**El resto de los usuarios podrán comprobar que el emisor es el legítimo propietario de los criptoactivos utilizando la clave pública [...].**

- **Autentificación del emisor:** para que el emisor pueda firmar el mensaje y la red pueda comprobar la titularidad de los activos, deberá firmar con su clave privada. El resto de los usuarios podrán comprobar que el emisor es el legítimo propietario de los criptoactivos utilizando la clave pública para descifrar el mensaje previamente encriptado con la clave privada. Es decir, si el mensaje es descifrado por la red utilizando la clave pública, querrá decir que el mensaje ha sido enviado de forma fehaciente por quien dice ser el emisor o, al menos, por alguien que dispone de su clave secreta. Por ejemplo, si un usuario quiere realizar una transacción, deberá indicar en el mensaje su clave pública para identificarse, la cantidad de bitcoines que desea enviar y la clave pública

del destinatario. Además, deberá firmar (encriptar) el mensaje con su clave privada. El resto de los usuarios podrán desencriptar el mensaje con la clave pública del emisor y comprobar que este es el usuario que dice ser con la clave pública (Conesa, 2019).

La novedad más importante de las redes de registro descentralizado *blockchain* consiste en la creación de una cadena de bloques que sirve de base de datos para validar y registrar las transacciones de criptomonedas que se efectúan entre los usuarios. Es decir, con la creación de un bloque se pretenden validar y registrar en una base de datos disgregada una multitud de operaciones. Al ser una red descentralizada, serán algunos usuarios, movidos por la posibilidad de obtener una recompensa, los que los crearán y almacenarán en sus propios servidores. Cualquiera de los usuarios puede acceder a la información de los bloques almacenada en diferentes servidores a través de las conexiones múltiples existentes en la red. Cada uno de estos bloques contiene la siguiente información (Conesa, 2019; Dolader *et al.*, 2017):

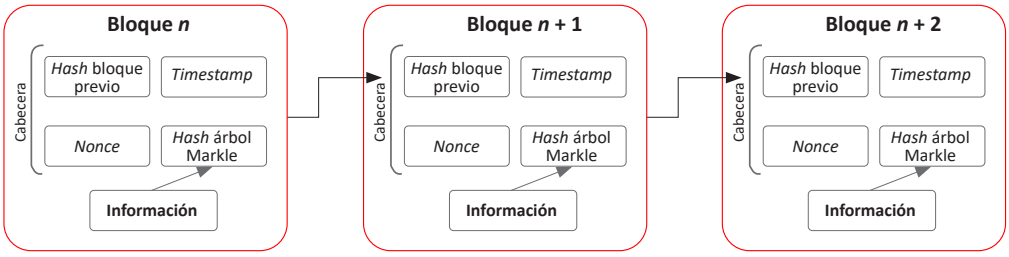
**La novedad más importante de las redes de registro descentralizado *blockchain* consiste en la creación de una cadena de bloques que sirve de base de datos para validar y registrar las transacciones [...].**

- La marca de tiempo (fecha y hora exacta en la que se crea el bloque) y el número de bloque que ocuparía en la serie.
- La referencia al bloque anterior. Se utiliza un algoritmo criptográfico denominado *hash*, que asigna un código de referencia concreto al contenido del bloque anterior. Este código garantiza la seguridad de las operaciones y la imposibilidad de modificar el contenido de bloques anteriores, ya que cada nuevo bloque contiene el código *hash* del anterior bloque y así sucesivamente. Cualquier información concreta (entrada) se convierte en una combinación de números y letras de longitud fija: el referido código *hash* (salida). Un mismo e idéntico contenido siempre dará como resultado el mismo *hash*. Si se produce cualquier modificación del contenido de la entrada, por pequeña que sea, la función generará uno totalmente diferente. Del mismo modo, es imposible que dos entradas distintas puedan generar un código idéntico. Además, se trata de una función no reversible, es decir, es imposible hallar el contenido de la entrada a partir del *hash*.

**Al ser una red descentralizada, serán algunos usuarios, movidos por la posibilidad de obtener una recompensa, los que los crearán y almacenarán en sus propios servidores.**

- La información relativa al conjunto de transacciones que se pretende verificar. Para reforzar la seguridad y la inmutabilidad de la información almacenada, cada una de las operaciones tiene asignada un código *hash*. Estos códigos se irán agrupando hasta formar un único *hash* asignado al conjunto de operaciones existentes en el bloque.
- La solución de la prueba algorítmica que sirve de mecanismo consensual y que se explica en el siguiente apartado. Su resultado se denomina *nonce*.
- De esta manera, los bloques quedan ligados de forma lineal y ordenados de forma cronológica.

**Figura 3. Estructura de los bloques de la *blockchain***




Fuente: Basado en el principio de Dolader *et al.* (2017).

En resumen, la tecnología *blockchain* consiste en la creación de una cadena de bloques como base de datos segura e inmutable por parte de una red de usuarios que se relacionan en un plano de igualdad y que verifican su identidad a través de claves criptográficas. Cada uno de estos bloques contiene información de un conjunto de transacciones, así como la referencia al bloque anterior. Además, la incorporación de un nuevo bloque se materializa una vez superado un mecanismo de consenso —en el caso de Bitcoin consiste en una prueba de trabajo *(proof of work)*— que trata de buscar la solución a un problema algorítmico que imposibilita a los usuarios crear bloques fraudulentos y se explica a continuación.

## 2.3. MECANISMOS DE CONSENSO Y MINADO DE CRIPTOMONEDAS

Una de las características esenciales del sistema de pagos de las criptomonedas consiste en la validación y el registro de las operaciones de forma descentralizada. Se mantiene como referencia el funcionamiento de Bitcoin, aunque existen múltiples variables en cuanto al mecanismo de consenso. Cuando un usuario de la red ordena una operación, ya sea de compra o de venta de activos, esta se considerará efectuada en el momento en que se valide y registre en la plataforma. Este proceso de validación y registro, que se denomina *minado*, se realiza una vez que se ha incorporado la transacción a un nuevo bloque (recuérdese que cada uno de los bloques valida y registra un conjunto de operaciones).

**Cualquier usuario de la red puede aspirar a validar y registrar un conjunto de transacciones mediante la creación de un bloque nuevo en la cadena, que tendrá como recompensa la adquisición de nuevas criptomonedas.**

Cualquier usuario de la red puede aspirar a validar y registrar un conjunto de transacciones mediante la creación de un bloque nuevo en la cadena, que tendrá como recompensa la adquisición de nuevas criptomonedas. Dicha recompensa —que se recibe en forma de activos— es la motivación que impulsa a muchos usuarios a tratar de competir para la creación de nuevos bloques y la validación de transacciones. La denominación de este proceso responde a la existencia de múltiples paralelismos con el minado del oro. El usuario que pretende crear nuevos bloques, también llamado minero, deberá seleccionar aquellas operaciones que desea validar. Con carácter previo, tendrá que verificar su legitimidad, esto es, comprobar la autenticidad del emisor, que este dispone de fondos y que no se ha duplicado la operación. A continuación, introducirá la información de las transacciones seleccionadas en el bloque, además de la asignación de la recompensa a su favor (Berentsen y Schar, 2018; Conesa, 2019; Dolader, Bel y Muñoz, 2017).

**Como mecanismo de consenso, el minero tiene que resolver una prueba para que su bloque sea el que se incorpore a la cadena.**

Como mecanismo de consenso, el minero tiene que resolver una prueba para que su bloque sea el que se incorpore a la cadena. Es decir, varios usuarios de la red compiten de forma simultánea para conseguir que el bloque que han creado —en el cual se incluye la validación de un conjunto de transacciones— sea el que se incorpore a la cadena

existente. Ya se ha indicado en el epígrafe anterior que el nuevo bloque debe contener el número que ocuparía en la serie, la marca de tiempo, el código *hash* del bloque anterior, la información relativa a las transacciones y un valor denominado *nonce*, que será el resultado obtenido tras la prueba criptográfica realizada por el minero. El primer minero que consiga resolver la prueba criptográfica será el que incorpore el bloque que previamente ha creado y obtendrá, además, la recompensa en forma de activos creados *ex novo* y de forma específica en ese proceso; de ahí que esta fase se denomine *minado*. Los demás usuarios comprobarán la validez de las transacciones y que la resolución de la prueba es correcta. Acto seguido, acordarán de forma consensuada que el bloque en cuestión es el que se debe añadir a la cadena e iniciarán de nuevo el proceso de creación de nuevos bloques con las transacciones pendientes de validar. De esta manera, se genera un mecanismo de consenso y se emiten nuevos activos que se asignarán al usuario que ha conseguido superar en primer lugar la prueba (Berentsen y Schar, 2018; Conesa, 2019).

**El primer minero que consiga resolver la prueba criptográfica será el que incorpore el bloque que previamente ha creado y obtendrá, además, la recompensa [...].**

Esta prueba criptográfica diseñada para el bitcóin y utilizada por muchas otras criptomonedas se denomina *prueba de trabajo (proof of work)*. Consiste en hallar el resultado de una función matemática que solo es posible resolver si se utiliza la fuerza bruta computacional. Tal como se ha mencionado, cada bloque tiene asignado un código *hash* determinado, generado con toda la información que aquel contiene. Pues bien, la prueba exige que el valor *hash* del bloque incluya en sus primeros dígitos varios ceros, de modo que los usuarios deberán hallar el valor denominado *nonce* (resultado de la prueba) que haría que el código *hash* comience según ese criterio. Para ello, dado que no es posible resolver esta función con una fórmula matemática, el minero deberá probar diferentes combinaciones con la fuerza bruta de su computadora, hasta obtener el valor que correspondería al *nonce* para que, junto con el resto de la información contenida en el bloque, dé como resultado un *hash* que comience por un número determinado de ceros. Cuando obtiene una solución, el minero la publica en la red para que todos los usuarios comprueben que tanto la validación de las transacciones como la prueba de trabajo se han realizado correctamente; acto seguido, se incorpora el bloque a la cadena (Berentsen y Schar, 2018; Conesa, 2019).

**Consiste en hallar el resultado de una función matemática que solo es posible resolver si se utiliza la fuerza bruta computacional.**

Cada bloque contiene la información relativa a muchas transacciones, lo que dificulta la posibilidad de hallar el valor *nonce* con pocas combinaciones. Los mineros necesitan potentes computadoras que consumen mucha energía para resolver esta prueba criptográfica. El elevado gasto energético ha sido muy cuestionado, cuestión que se aborda en el apartado relativo al impacto medioambiental.

## 2.4. TIPOS DE CRIPTOMONEDAS

Según señala el portal web CoinMarketCap, a lo largo de estos años se han creado más de 21.000 criptomonedas diferentes y, hoy en día, se mantienen activas en torno a 10.000, las cuales operan en distintas plataformas de tecnología de registro descentralizado. En la siguiente figura se incluyen las 10 más importantes por orden de capitalización de mercado.

**Figura 4. Las 10 principales criptomonedas según su capitalización de mercado**

| # | Nombre | Precio | 1h % | 24h % | 7d % | Cap. de Mercado | Volumen (24h) | Acciones en circulación |
|---|---|---|---|---|---|---|---|---|
| 1 | Bitcoin BTC | $19,412.72 | 0.24% | 1.19% | 0.03% | $371,850,332,510 | $28,719,151,365<br>1,481,951 BTC | 19,188,025 BTC |
| 2 | Ethereum ETH | $1,348.20 | 0.61% | 2.97% | 1.90% | $164,658,004,721 | $12,620,201,537<br>9,379,336 ETH | 122,373,863 ETH |
| 3 | Tether USDT | $1 | 0.00% | 0.01% | 0.01% | $68,461,677,742 | $39,187,898,178<br>39,182,992,820 USDT | 68,453,108,029 USDT |
| 4 | BNB BNB | $274.79 | 0.27% | 1.81% | 0.84% | $43,933,061,605 | $547,455,223<br>1,993,534 BNB | 159,980,276 BNB |
| 5 | USD Coin USDC | $1 | 0.00% | 0.00% | 0.01% | $43,889,519,649 | $2,757,691,114<br>2,757,822,204 USDC | 43,891,605,981 USDC |
| 6 | XRP XRP | $0.4575 | 0.79% | 0.35% | 2.51% | $22,768,368,047 | $1,279,791,655<br>2,804,109,028 XRP | 49,887,015,710 XRP |
| 7 | Binance USD BUSD | $0.9997 | 0.05% | 0.01% | 0.10% | $21,637,973,233 | $5,389,487,349<br>5,387,028,322 BUSD | 21,628,100,611 BUSD |
| 8 | Cardano ADA | $0.3621 | 0.24% | 3.60% | 2.24% | $12,395,785,454 | $408,102,935<br>1,129,414,767 ADA | 34,305,029,297 ADA |
| 9 | Solana SOL Comprar | $28.93 | 0.97% | 2.09% | 5.55% | $10,342,304,837 | $698,283,960<br>24,196,365 SOL | 358,373,095 SOL |
| 10 | Dogecoin DOGE Comprar | $0.05977 | 0.49% | 0.57% | 0.60% | $7,918,568,433 | $220,648,793<br>3,696,835,391 DOGE | 132,670,764,300 DOGE |

Fuente: Coin Market Cap. (2022). Último acceso el 24 de octubre del 2022.

Existen diferentes tipos de criptomonedas. Es posible establecer una primera clasificación en atención a la funcionalidad del activo y una segunda que las diferencia en función de si su valor depende exclusivamente de la oferta y la demanda del mercado (como el bitcóin) o si, por el contrario, este está referenciado al de otro activo más estable *(stablecoins)*.

**A partir del 2017, surgieron nuevas criptomonedas que, además de ejercer las funciones clásicas del dinero, se convertían en activos con derechos adicionales.**

## Funcionalidad de las criptomonedas

A partir del 2017, surgieron nuevas criptomonedas que, además de ejercer las funciones clásicas del dinero, se convertían en activos con derechos adicionales. Así pues, una primera clasificación responde a la naturaleza o funcionalidad de los activos digitales. Tenemos *tokens* de pago, de inversión o seguridad y de utilidad (Otero y Oliver, 2022; PwC, 2019):

- **Activos de pago *(payment tokens).*** Se limitan a ejercer las funciones clásicas de las monedas o alguna de ellas: servir como medio de pago, como depósito de valor y como unidad de cuenta.
- **Activos de inversión *(security tokens).*** Son la representación de un instrumento financiero, por lo que permiten a sus propietarios ejercer los derechos correspondientes a activos financieros, como acciones, obligaciones u otros activos de inversión.
- **Activos de utilidad *(utility tokens).*** Disponen de una utilidad concreta y otorgan un derecho en el marco de un contrato inteligente *(smart contract)*. Por ejemplo, dan a su propietario el derecho a acceder a una aplicación o un servicio, a obtener un bien o a recibir un pago. Es decir, el activo digital lleva aparejada la ejecución de un determinado derecho, en el marco de un contrato, si se cumplen una serie de requisitos.

### *Stablecoins*

Se puede establecer una segunda clasificación de las criptodivisas en función de la fluctuación o estabilización de su valor. Así, cabe diferenciar aquellas criptomonedas convencionales en las que el valor depende exclusivamente de la oferta y la demanda (como el bitcóin), de una nueva subcategoría de criptomonedas denominadas *stablecoins*, cuyo valor se encuentra vinculado al precio de otro activo o cesta de activos subyacentes. Esta última subcategoría de criptodivisas, que ha surgido en los últimos años, pretende reducir la volatilidad mediante la estabilización de su precio, con la finalidad de que puedan ser aceptadas con mayor facilidad como medio de pago. Encontramos los siguientes tipos de *stablecoins* en función del activo al que van referenciadas (PwC, 2021):

- **Vinculadas a materias primas.** Están vinculadas a activos físicos, generalmente metales preciosos como el oro o la plata. Para que su vinculación sea efectiva, requiere que la emisión de la criptomoneda se encuentre respaldada por reservas del material al que va vinculado.
- **Vinculadas a monedas fíat.** Se hallan respaldadas por reservas de monedas oficiales de Estados soberanos y, en particular, por aquellas divisas que cuentan con mayor aceptación, seguridad y estabilidad. Aprovechan la credibilidad que proporciona el respaldo de un banco central. Por ejemplo, tether (USDT) es una criptomoneda que se emite en las *blockchain* de Bitcoin y Ethereum y funciona como una *stablecoin* anclada al dólar estadounidense, aunque también dispone de versiones ancladas a otras monedas como el euro o, incluso, al oro (Otero y Oliver, 2022).
- **Vinculadas a otras criptodivisas.** Su valor está ligado al de otras criptomonedas. En general, se puede garantizar su respaldo mediante un registro *on-chain* (en la propia red *blockchain*), a través del cual los propios usuarios pueden comprobar la existencia de reservas de la criptomoneda a la que está vinculada.
- **Vinculadas a una cesta de activos.** Referencian su valor al de una combinación de diferentes tipos de activos.

**[...] cabe diferenciar aquellas criptomonedas convencionales en las que el valor depende exclusivamente de la oferta y la demanda [...] de una nueva subcategoría de criptomonedas denominadas *stablecoins*, cuyo valor se encuentra vinculado al precio de otro activo [...].**

En el 2019, Facebook anunció la creación de Libra 2.0, una combinación de *stablecoins* privadas y un sistema global de pago electrónico. El ambicioso proyecto pretendía la emisión de estos activos vinculados a las principales divisas y la creación de una *stablecoin* global vinculada a la cesta de los demás criptoactivos. Todos estos ellos operarían en Libra *Blockchain*, un sistema para proveer servicios de pago. Además, la moneda global libra 2.0 estaría disponible para otros clientes y redes (Arner *et al.*, 2020). Este proyecto, que se vio forzado a rebajar algunas de sus propuestas y a cambiar su nombre a *Diem* por la retirada de la confianza de empresas colaboradoras, finalmente no vio la luz. Los Estados y organismos internacionales mostraron su reticencia a que una empresa privada con la red de usuarios más grande del planeta pudiera crear una especie de moneda digital global, fuera del control de los Gobiernos y con un elevado riesgo de contagio al sistema financiero mundial (Otero y Oliver, 2022).

También ha surgido un tipo de *stablecoins* en las que no es necesario el respaldo de los activos vinculados, pues el precio se estabiliza de forma automática a través de algoritmos previamente programados. Este tipo de activos pretenden mantener su valor ligado al de una divisa fíat u otro criptoactivo, controlando el número de monedas en circulación a través de la mayor o menor emisión de nuevos activos. Este tipo de medidas, similares a las que adoptaría un banco central respecto de una moneda nacional, se aplican de forma automática cuando se dan una serie de circunstancias, mediante órdenes de emisión

de nueva moneda previamente programada a través de fórmulas algorítmicas. Un ejemplo sería terra USD, una criptomoneda que trataba de mantener su valor vinculado al dólar estadounidense. Su estabilización se alcanzaba a través de otra criptomoneda hermana, luna, que ejercía la función de ancla en el intercambio de terra USD por dólares norteamericanos. Esta última criptomoneda implosionó en mayo del 2022, perdiendo el 99% de su valor debido a la retirada de la confianza por parte de usuarios e inversores. Desde entonces, la credibilidad de este tipo de *stablecoins* ha disminuido (BPI, 2022).

**[...] si bien las *stablecoins*, a diferencia de las criptomonedas sin respaldo, pueden conseguir la estabilización de su valor, siguen careciendo de las cualidades necesarias para erigirse como sistema monetario alternativo [...].**

En todo caso, si bien las *stablecoins*, a diferencia de las criptomonedas sin respaldo, pueden conseguir la estabilización de su valor, siguen careciendo de las cualidades necesarias para erigirse como sistema monetario alternativo por sí mismas, ya que, en general, recurren a la confianza que generan las propias monedas fíat u otros activos tradicionales; además, los usuarios no pueden beneficiarse de la regulación y de la protección a los depósitos y a la liquidez que establecen las autoridades centrales respecto a sus monedas tradicionales (BPI, 2022).

Estos casos ponen de manifiesto algunos de los problemas éticos que surgen en relación con las criptomonedas y que se analizan en el siguiente apartado.

# 3. RIESGOS ÉTICOS DE LAS CRIPTOMONEDAS

Hasta aquí se ha tratado de explicar, de la forma más sencilla posible, la naturaleza, las características y las tipologías de las criptomonedas, además de exponer su complejo funcionamiento. En los siguientes epígrafes se abordan los distintos riesgos asociados a la ética en relación con este tipo de divisas digitales basadas en la tecnología de registro descentralizado y que pretenden construir un sistema monetario alternativo al vigente. En concreto, abordamos el carácter especulativo de muchas de las criptomonedas; los problemas relacionados con la seguridad, la transparencia o las actividades delictivas; la adicción que están provocando en muchos jóvenes; y, por último, el impacto medioambiental derivado de la tecnología *blockchain*.

## 3.1. USO ESPECULATIVO

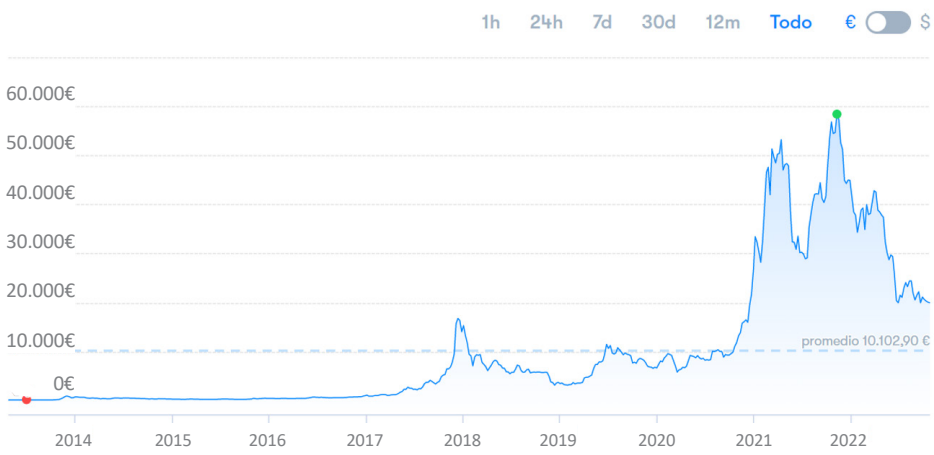
**Algunos autores sugieren que la especulación forma parte de la naturaleza de la mayoría de las criptomonedas, las cuales requieren de este comportamiento para su funcionamiento.**

Uno de los principales riesgos de la mayoría de las criptomonedas es su elevada volatilidad y su dependencia de las expectativas de compradores y vendedores en transacciones futuras, fruto de la propia especulación por parte de muchos de los usuarios (Banco de España, 2022). Un estudio señala que el 90% de las transacciones de Bitcoin no se corresponden con actividades económicamente relevantes y que el 75% se debe a la mera especulación. Las *stablecoins*, pese a buscar un valor nominal estable, tampoco se escapan de la fiebre especulativa y han sufrido graves problemas de estabilidad (Makarov y Schoar, 2021). Algunos autores sugieren que la especulación forma parte de la naturaleza de la mayoría de las criptomonedas, las cuales requieren de este comportamiento para su funcionamiento. Al respecto, argumentan que el minado y la validación de transacciones exige cubrir unos costes en tecnología y electricidad que no pueden pagarse con las propias criptomonedas, ya que estas no son aceptadas de forma general como medio de pago; por ello, los mineros necesitan intercambiar sus criptoactivos por dinero fiduciario una vez recibida su recompensa. Para que ese intercambio sea posible, la compra de los activos digitales tiene que ser atractiva para los inversores, es decir, debe generar confianza y la expectativa de que su valor subirá en el futuro. Por tanto, con el fin de que los mineros puedan hacer frente a los costes derivados de su trabajo, es preciso garantizar la continua entrada de especuladores que estén dispuestos a intercambiar dinero fiduciario por criptomonedas con la perspectiva de que su valor continúe aumentando (Otero y Oliver, 2022).

**[...] es el propio carácter especulativo, ligado a la volatilidad, el que aleja a la mayoría de las criptomonedas de ejercer las funciones clásicas del dinero.**

La naturaleza especulativa de la mayoría de las criptomonedas ha recibido numerosas críticas desde el campo de la economía y las finanzas, ya que genera deflación —que impide que sean utilizadas como reserva de valor— y una elevada volatilidad —que puede suponer el estallido de una burbuja económica— (Bagus y De la Horra, 2021). Un artículo publicado por CaixaBank Research señalaba, ya en el 2018, que la evolución del bitcóin estaba marcada por un bum de precios que iba mucho más allá de su utilización y por la euforia emocional, circunstancias que encajan bastante bien con las fases iniciales de una burbuja especulativa identificadas por Kindleberger y Minsky (Fernández, 2018). De hecho, es el propio carácter especulativo, ligado a la volatilidad, el que aleja a la mayoría de las criptomonedas de ejercer las funciones clásicas del dinero. En este sentido, O'Neill (2021) se pregunta por qué se debería otorgar la condición de dinero a una "fuerza anónima o amorfa como un registro descentralizado que limita la oferta total de la moneda y garantiza así su perpetua volatilidad".

**Figura 5. Los precios del bitcóin**




Fuente: Tomado de BTCdirect.eu. Recuperado el 24 de octubre de 2022 (valor de bitcoin en miles de euros).

Un estudio del Banco de Pagos Internacionales (BPI) considera que la elevada volatilidad del valor de las criptomonedas responde a la ausencia de una autoridad central que garantice su estabilidad. Al no disponer de esta, no puede expandir o contraer su balance general y, por tanto, cualquier oscilación en la demanda de los activos fruto de la especulación se traduce en la fluctuación de su valor. La continua proliferación de nuevas criptomonedas tampoco ayuda a estabilizar el valor de las ya existentes (BPI, 2018). Otro estudio del mismo organismo concluye que las criptomonedas resultan inútiles para efectuar pagos. Ni siquiera son vistas por la mayoría de sus usuarios como alternativa a las monedas fíat o a las finanzas reguladas, sino como un mero activo de inversión a través del cual especular. Por ello, los autores del estudio defienden que deberían someterse a la regulación y supervisión de los mercados financieros y de los servicios de inversión (Auer y Tercero-Lucas, 2021).

**[...] existe una diferencia sustancial desde el punto de vista moral entre invertir y especular.**

Cabría plantearse entonces la utilidad de las nuevas monedas digitales y si su carácter puramente especulativo es beneficioso para la sociedad. El filósofo Michael Sandel, conocido por sus libros y cursos divulgativos sobre justicia y filosofía pública, señaló en un artículo publicado en el 2013 que existe una diferencia sustancial desde el punto de vista moral entre invertir y especular. Aunque ambas acciones comportan arriesgar dinero con la esperanza de obtener un beneficio, invertir promueve la producción de bienes y servicios que son útiles para la sociedad, mientras que especular consiste en hacer dinero al tratar de acertar sobre futuros precios o eventos, sin producir bienes o servicios ni aportar nada útil a la sociedad. Sandel sostiene que la especulación no solo puede comportar daños individuales (como pérdidas económicas o adicciones), sino que también es perjudicial para el bien común y para las actitudes y virtudes que hacen a una sociedad justa, pues se rompe la frágil conexión entre contribución y compensación, entre trabajo y rendimientos, y entre personas que trabajan sin apenas recompensa y personas que adquieren beneficios sin apenas esfuerzo (Sandel, 2013). En este sentido, siguiendo su razonamiento, el carácter puramente especulativo de las criptomonedas estaría dañando la justicia y el bien común.

**Sandel sostiene que la especulación no solo puede comportar daños individuales (como pérdidas económicas o adicciones), sino que también es perjudicial para el bien común y para las actitudes y virtudes que hacen a una sociedad justa [...].**

Además, otro elemento que debe tenerse en cuenta es que el crecimiento que ha experimentado la inversión en criptomonedas en cuanto activos puramente especulativos disminuye la posibilidad de invertir esos recursos en la economía real, en activos o bonos ligados a empresas productivas o, incluso, en proyectos que generen impacto positivo en la sociedad y en el medioambiente (Conklin y Ceballos, 2022).

## 3.2. SEGURIDAD, TRANSPARENCIA Y PREVENCIÓN DE DELITOS

La tecnología *blockchain* convierte a las criptomonedas en un sistema de registro de transacciones realmente seguro y fiable, prácticamente imposible de alterar o falsificar, debido al encadenamiento de bloques con técnicas criptográficas. Este mecanismo —uno de sus indudables puntos fuertes frente al sistema tradicional de pagos— no garantiza una seguridad completa para el usuario final, ya que este puede sufrir el robo de su clave privada —único elemento de identificación— a través del hackeo de su monedero digital, la aplicación donde habitualmente se guardan las claves (Europol, 2021). A diferencia de las operaciones de pago del sistema bancario, las transacciones realizadas a través de una clave robada no cuentan con una protección que reintegre los fondos perdidos (Conesa, 2019). Es decir, aunque se sirven de una tecnología cien por cien segura que impide la falsificación de las transacciones en la base de datos, existen otro tipo de vulnerabilidades en la custodia de las claves privadas en los monederos digitales, frente a las cuales no hay, además, una regulación que proteja a la víctima o usuario final.

**Este anonimato en la red, que puede tener su razón de ser en la propia publicidad del registro, comporta serios riesgos y dificultades para prevenir y combatir delitos como el blanqueo de capitales, la evasión fiscal o la financiación de actividades ilegales [...].**

La descentralización de la tecnología *blockchain* ha traído también la transparencia de la red y del registro de transacciones. Muchos de los partidarios de las criptomonedas sugieren que esta característica se opone a la opacidad de un sistema centralizado. La transparencia es posible gracias al anonimato de los usuarios. Es decir, estos operan a través de dos tipos de claves: una pública que sirve de identificación, como una especie de número de cuenta IBAN, y una privada que deben custodiar los propios usuarios (quienes, con frecuencia, lo hacen a través de monederos digitales o casas de cambio); pero en ningún caso queda registrada en la red *blockchain* la asociación de las claves con la identidad real del usuario. Este anonimato en la red, que puede tener su razón de ser en la propia publicidad del registro, comporta serios riesgos y dificultades para prevenir y combatir delitos como el blanqueo de capitales, la evasión fiscal o la financiación de actividades ilegales, de terrorismo, de organizaciones mafiosas o, incluso, de guerras. Ahora bien, también es cierto que el anonimato en algunos casos no es del todo completo, ya que muchos de los usuarios se identifican ante intermediarios como casas de cambio al realizar operaciones de canje de bitcoines por monedas nacionales (Conesa, 2019).

Aunque en la mayoría de los casos no se puede alcanzar el anonimato total, sí es posible que se efectúen con mayor facilidad transacciones ilegales para cometer o financiar delitos como los señalados con anterioridad. Los distintos actores que operan en el sector bancario y financiero tienen la obligación de identificar a sus clientes a través del procedimiento Know Your Costumer (KYC) ('Conozca a su cliente'), una serie de controles que tienen como finalidad identificar y registrar a todos los clientes, además de vigilar que las transacciones no tengan fines criminales, que la procedencia de los fondos sea lícita y que no se evadan impuestos. Si bien existen diferentes iniciativas regulatorias comunitarias y nacionales (las directivas anti blanqueo de capitales, el Real Decreto Ley 7/2021 o la Ley 11/2021) que obligan a los intermediarios que gestionan el cambio de divisas por criptomonedas a identificar a los usuarios, muchas de las redes o bases de datos de criptomonedas escapan hoy en día del mencionado control y, además, algunas de las casas de cambio o intermediarios pueden operar desde centros financieros *offshore*, lo cual facilita el blanqueo de capitales, la evasión fiscal o la comisión de otros delitos (Otero y Oliver, 2022).

Las criptomonedas y, en especial, el bitcóin, debido a su casi anonimidad, se han utilizado como instrumento o medio de pago en redes descentralizadas de mercado negro *online (darknet)*, en las que usuarios pueden operar a través de protocolos de comunicación que garantizan su anonimato. Además, el auge de las criptomonedas a nivel global ha supuesto una internacionalización de los mencionados mercados negros que ven como

pueden llegar a más personas y proteger sus comunicaciones a través la tecnología *blockchain* y la criptografía. En el 2013, el FBI cerró el portal Silk Road, un *market place online* de compraventa de drogas y pornografía infantil mediante criptomonedas, cuyo cierre provocó la propia caída del bitcóin. En este sentido, un estudio realizado por académicos de la University of Sydney sugiere que el valor intrínseco del bitcóin, más allá de la especulación, se debe en gran medida a la posibilidad de realizar actividades ilícitas, de tal manera que el cierre de portales de internet que facilitan el comercio negro provoca una caída en el valor de la criptomoneda utilizada por estos. El estudio también sostiene que las actividades delictivas representan el 46% de las transacciones en bitcoines. Pese a que las criptomonedas han facilitado la actividad en ese mercado negro, algunos autores defienden que la propia publicidad y la transparencia de la red *blockchain* permiten la trazabilidad de las operaciones, al detectar la IP desde la que se han cometido delitos (Conklin y Ceballos, 2022; Foley *et al.*, 2019; Otero y Oliver, 2022).

Otra actividad delictiva que afecta al mercado de las criptomonedas es el fraude cometido por intermediarios que operan a través de estructuras opacas y que pretenden captar inversores con la falsa promesa de obtener elevados rendimientos. Seducen a posibles víctimas utilizando información obtenida en las redes sociales y manipulan *software* para mostrar atractivas recompensas. Estas redes operan muchas veces bajo el método de la estafa piramidal e incluso, en ocasiones, consiguen capital de los usuarios para invertir en criptomonedas que ni siquiera existen (Europol, 2021).

**Otra actividad delictiva que afecta al mercado de las criptomonedas es el fraude cometido por intermediarios que operan a través de estructuras opacas y que pretenden captar inversores con la falsa promesa de obtener elevados rendimientos.**

Las actividades delictivas a través de criptomonedas no parecen disminuir. Un informe de la Europol advierte del aumento de la comisión de todo tipo de delitos que utilizan las criptomonedas a través de complejas y sofisticadas redes o estructuras que operan en las plataformas *blockchain*. Aunque en el 2021 se alcanzó cifra récord de 14.000 millones de dólares vinculados a actividades delictivas, el porcentaje respecto al total de transacciones realizadas con activos digitales disminuyó debido al enorme crecimiento que experimentó el mercado de las criptomonedas, fruto de la especulación. En muchas ocasiones, el blanqueo de capitales o la financiación de actividades ilícitas se produce a través de intermediarios que prestan servicios anidados *(nested services)*; estos servicios cuentan con una normativa KYC laxa o nula que garantiza la opacidad y el anonimato y, además, impiden la trazabilidad de las transacciones ya que permiten adquirir la propiedad de los activos de sus usuarios y confundir sus fondos (Europol, 2021; Makarov y Schoar, 2021).

### 3.3. PROBLEMAS DE ADICCIÓN ENTRE LOS MÁS JÓVENES

Otro gran reto para el mercado de las criptomonedas es la adicción que, en pleno boom especulativo —coincidiendo con la crisis de la COVID-19, en un contexto de gran incertidumbre económica, paro juvenil y precariedad laboral—, ha generado entre numerosos jóvenes, los cuales se ven seducidos por la promesa de obtener elevados y generosos rendimientos.

**[...] los jóvenes invierten sus ahorros y asumen elevados riesgos sin apenas comprender el funcionamiento económico, financiero o tecnológico de las criptomonedas.**

El carácter aparentemente transgresor del mundo de las criptomonedas atrae a muchos de estos jóvenes. Otros adquieren sus primeras monedas digitales al estar familiarizados con la cultura de los videojuegos, el juego *online* o las apuestas deportivas. También desempeñan un papel fundamental al respecto los anuncios y la promoción en redes sociales por parte de *influencers* o famosos que presumen de haber obtenido grandes ganancias. Otro factor es la proliferación de aplicaciones móviles o webs con un diseño sencillo y atractivo que promueven cursos fáciles de finanzas impartidos por instructores sin apenas formación en economía y que dicen garantizar un rápido enriquecimiento. En todos estos casos, los jóvenes invierten sus ahorros y asumen elevados riesgos sin apenas comprender el funcionamiento económico, financiero o tecnológico de las criptomonedas. Incluso, en

muchas ocasiones, recurren al endeudamiento con la ingenua esperanza de hacerse ricos. Además, la mayoría opera a través de intermediarios que no cumplen con la normativa equivalente para los mercados de divisas y valores tradicionales, por lo que las inversiones realizadas no se encuentran protegidas por el marco regulatorio de garantías y salvaguardas de las finanzas tradicionales (Otero y Oliver, 2022).

Factores como la posibilidad de comprar y vender activos en cualquier momento, la instantaneidad de las inversiones, el atractivo de la figura y el estatus del inversor, la dependencia de la tecnología o la adrenalina que genera la asunción de riesgos son un caldo de cultivo perfecto para que surjan adicciones a las criptomonedas por parte de los jóvenes. Entre los síntomas de esa adicción se encuentran la ansiedad, la depresión, la irritabilidad, la pasividad en las relaciones sociales, el abandono de los estudios y el endeudamiento (Serrano, 2021).

**[...] la posibilidad de comprar y vender activos en cualquier momento, la instantaneidad de las inversiones, el atractivo de la figura y el estatus del inversor, la dependencia de la tecnología o la adrenalina que genera la asunción de riesgos son un caldo de cultivo perfecto para que surjan adicciones [...].**

En el origen de la adicción de los jóvenes a las criptomonedas también se encuentran organizaciones fraudulentas y sectarias que actúan como supuestos intermediarios y dicen ofrecer cursos de formación, pero en realidad son chiringuitos financieros (pues ofrecen servicios financieros sin licencia) que tratan de captar jóvenes, especialmente adolescentes de entre 14 y 20 años; operan como estafas piramidales (las supuestas ganancias proceden únicamente de la incorporación de nuevos usuarios, de tal manera que cuando no se incorporan suficientes nuevos miembros el esquema estalla y los usuarios pierden su dinero); y, además, actúan con métodos sectarios: los alejan de sus familias, les aconsejan abandonar estudios y trabajo para centrarse exclusivamente en la organización, les facilitan información manipulada y los utilizan para captar nuevos usuarios. Es decir, no solo crean una adicción a multitud de adolescentes y jóvenes, sino que, además, los estafan y los abducen como si de una secta se tratara. La Comisión Nacional del Mercado de Valores (CNMV) aconseja desconfiar de las organizaciones que insisten en la urgencia de invertir para no perder oportunidades únicas, en aportar nuevos fondos o en captar nuevos usuarios (Ramírez, 2022). En España, la Policía Nacional detuvo en marzo del 2022 a ocho personas de una organización denominada IM Academy, que está siendo investigada por estafar a través de cursos virtuales y transacciones financieras de alto riesgo. Pese a ello, esta polémica organización pudo celebrar el pasado mes de mayo un macroevento en Badalona con la participación de más de 10.000 jóvenes de todo el mundo (RTVE, 2022).

Existen ciertas similitudes entre la adicción al juego *online* o a las apuestas deportivas y la adicción a las criptomonedas. Al igual que en el juego, tienen un papel importante los elementos de suerte y oportunidad, las ganancias incoherentes y la elevada probabilidad de escasa rentabilidad para la mayoría de los inversores. Un estudio señala que la inversión en criptomonedas atrae al mismo perfil de personas que desarrollan adicción a los juegos *online*: hombres jóvenes con ingresos y estudios, aunque no necesariamente con formación en finanzas (Delfabbro *et al.*, King y Williams, 2021).

La psicóloga Consuelo Tomás, fundadora y directora del Instituto Valenciano de Ludopatía y Adicciones no Tóxicas, incide en la diferencia entre invertir de una manera racional, sensata y coherente a medio o largo plazo, basada en conocimientos y estableciendo controles, y especular buscando sustanciosos e inmediatos beneficios, sin aceptar pérdidas, e incluso solicitando préstamos para tratar de revertir dichas pérdidas. Considera que este tipo de comportamiento facilita la adicción a las criptomonedas, junto con otros factores de carácter personal (como la impulsividad, búsqueda de sensaciones, falta de motivación académica o laboral, aumento de la adrenalina, sentido de pertenencia al grupo, o confianza excesiva en cursos o personas de su entorno), familiares (búsqueda de aprobación y reconocimiento en el seno familiar, o en algunas ocasiones son los propios padres quienes aportan dinero para que sus hijos realicen las inversiones), o factores socioambientales (nuevas tecnologías que

favorecen el anonimato y el uso durante 24 horas al día, fácil accesibilidad, publicidad en redes sociales). En este sentido, advierte que es necesario detectar precozmente la adicción -más frecuente en jóvenes de 17 a 25 años y adultos de 35 a 45 años- y buscar ayuda con especialistas lo antes posible (Rodríguez, 2022).

El profesor de Psicología Jeremiah Weinstock, de la Saint Louis University, señala que los atractivos específicos de las criptomonedas radican en su incertidumbre, en su volatilidad y en la supuesta posibilidad de obtener elevadas ganancias de forma temprana y sin apenas esfuerzo. Además, considera que la volatilidad contribuye a generar problemas de autoestima, ansiedad y depresión, ya que los jóvenes usuarios observan cómo su patrimonio varía considerablemente cada día (Tecnopasion.net, 2022). Un artículo del *Washington Post* (Verma, 2022) señala que la adicción a las criptomonedas puede comportar insomnio, soledad y depresión o, incluso, convertirse en una adicción puente, es decir, abrir la puerta a otro tipo de adicciones relacionadas con el alcohol y las drogas.

**[...] la volatilidad contribuye a generar problemas de autoestima, ansiedad y depresión [...].**

En este sentido, un estudio publicado en la revista *Addictive Behaviors* (Delfabbro *et al.*, 2021) identifica diferentes síntomas o riesgos que derivan de la adicción a las criptomonedas:

- **Ilusión de control.** Muchos de los jóvenes que invierten en criptomonedas creen que a través de ciertas habilidades, estrategias o rituales es posible aumentar las probabilidades de obtener ganancias. Por ejemplo, en una tendencia alcista de los activos, aunque la mayoría se verán beneficiados, muchos pensarán que sus ganancias se deben principalmente al tipo de decisiones que han tomado.
- **Credibilidad otorgada a falsos expertos en redes sociales.** Aunque hay personas con formación financiera impartiendo cursos *online* y promocionando la inversión en criptomonedas, han proliferado también multitud de jóvenes que presumen de ser expertos en el mercado de criptoactivos, pero que no disponen de la adecuada formación; al contrario, disponen de información incompleta y deficiente e incluso divulgan información falsa o engañosa. La confidencialidad de las promociones hace creer a los usuarios que son los primeros en conocer la información. Además, los supuestos expertos presumen de haber obtenido grandes beneficios y muestran gráficos sobre las expectativas de crecimiento de los activos, lo cual genera en los usuarios una sensación de urgencia y una falsa necesidad de invertir a fin de no perder la oportunidad.
- **Angustia.** Un factor común a todo tipo de adicción es la excesiva preocupación que genera el devenir de la propia actividad. El comercio de las criptomonedas se convierte en una actividad absorbente y desplaza otro tipo de responsabilidades más importantes.

**Los usuarios pueden desarrollar un temor continuo a perder alguna de las oportunidades que pueda generar ganancias.**

- **Miedo a perder oportunidades.** Se trata de uno de los factores psicológicos más fuertes que aparece en el comercio de criptomonedas. Los usuarios pueden desarrollar un temor continuo a perder alguna de las oportunidades que pueda generar ganancias. Si observan que el valor de una criptomoneda que no han adquirido está incrementando, se sienten molestos por no haber invertido en ella y se ven en la necesidad de adquirir tales activos con la esperanza de que su valor continúe experimentando incrementos.
- **Arrepentimiento anticipado.** Muchos usuarios desarrollan un sentimiento de culpabilidad. Se arrepienten de la insensatez de haber vendido unos determinados activos que con posterioridad se han revalorizado (arrepentimiento por acción), pero también de no haber adquirido activos cuyo valor se ha incrementado (arrepentimiento por omisión).

**Bitcoin, Ethereum y otras plataformas de criptomonedas utilizan una prueba de trabajo que recompensa a quien ejerce una mayor fuerza bruta computacional.**

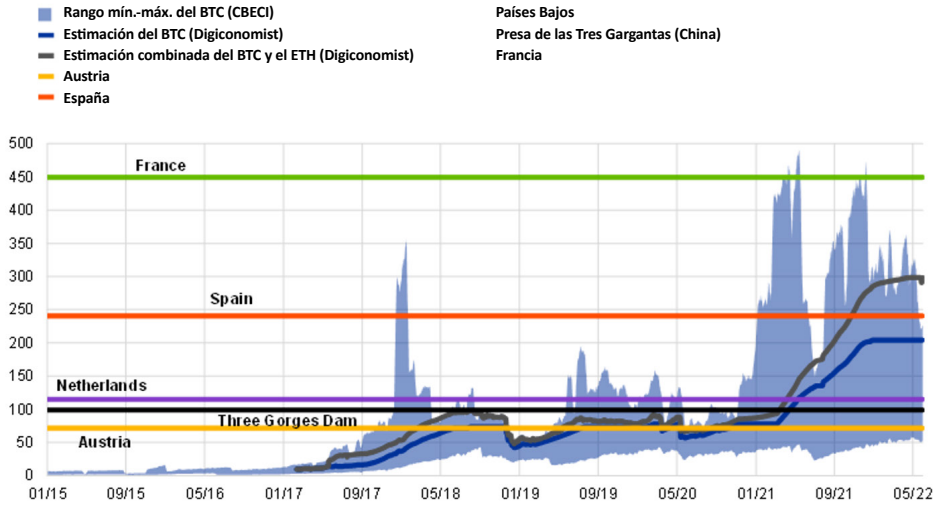
## 3.4. IMPACTO MEDIOAMBIENTAL

*A priori* podríamos pensar que la sustitución del dinero físico por activos digitales puede generar un impacto positivo, al reducir el consumo y la utilización de papel, plástico, metales u otros materiales necesarios para la confección de billetes, monedas o tarjetas. No obstante, en muchas ocasiones, la creación de criptomonedas y el registro electrónico de las transacciones requiere un importante consumo de energía.

El principal obstáculo que encuentran algunas criptomonedas desde el punto de vista medioambiental se halla en la propia tecnología *blockchain* y en la prueba consensual que requiere la validación de transacciones y la emisión de activos. Bitcoin, Ethereum y otras plataformas de criptomonedas utilizan una prueba de trabajo que recompensa a quien ejerce una mayor fuerza bruta computacional. En consecuencia, el proceso de minado es extremadamente costoso desde el punto de vista económico y exige un elevado y desmesurado consumo de energía que descarta cualquier tipo de sostenibilidad medioambiental de las criptomonedas que utilicen este mecanismo consensual de validación de transacciones (Gschossmann *et al.*, 2022). Pero, además, al margen de la prueba criptográfica, la propia lógica de la *blockchain* lleva aparejada un gasto de energía ascendente, pues exige la continua construcción de bloques nuevos referenciados al bloque anterior, sin que sea posible su reutilización, por lo que la propia tecnología en sí misma plantea una serie de retos en materia de sostenibilidad. Solo Bitcoin consume de forma anual la misma electricidad que países enteros como Holanda, Chile, Finlandia o Dinamarca, lo cual se traduce en más de 60 millones de toneladas de dióxido de carbono al año. A ello debe añadirse que el daño medioambiental causado por Bitcoin u otras plataformas de divisas digitales no aporta ningún beneficio importante ni para los usuarios ni para la sociedad, por lo que resulta totalmente prescindible (Conklin y Ceballos, 2022; Otero y Oliver, 2022).

**Solo Bitcoin consume de forma anual la misma electricidad que países enteros como Holanda, Chile, Finlandia o Dinamarca [...].**

**Figura 6. Consumo anual de electricidad estimado del bitcóin (BTC) y el ether (ETH) en comparación con el de determinados países**




Fuente: Gschossmann *et al.* (2022).

# 4. RECOMENDACIONES ÉTICAS PARA MEJORAR EL MODELO DE MONEDAS DIGITALES

Tras haber expuesto y desarrollado algunos de los problemas éticos que genera el mercado de las criptomonedas, vemos conveniente proponer algunas recomendaciones que pueden ayudar a paliar y reducir los riesgos identificados en el apartado anterior y transitar hacia un modelo de divisas digitales y de finanzas descentralizadas ético y sostenible.

## Inversión responsable

Un mercado puramente especulativo y que, además, permite el florecimiento de activos que no disponen de un valor real más allá de la financiación de actividades delictivas puede dañar la justicia y el bien común de una colectividad. Por ello, se considera necesario que desde la sociedad civil y los poderes públicos se fomente un tipo de inversión responsable, que contribuya a la producción de bienes o servicios o que aporte algún beneficio para la comunidad. En el campo de las criptomonedas, quizá sea recomendable invertir en aquellos activos que no responden a dinámicas exclusivamente especulativas y que disponen de un valor real o de una utilidad.

**En el campo de las criptomonedas, quizá sea recomendable invertir en aquellos activos que no responden a dinámicas exclusivamente especulativas y que disponen de un valor real o de una utilidad.**

Por otro lado, para evitar que los usuarios —especialmente los más jóvenes— puedan desarrollar adicciones, algunos expertos recomiendan ceñirse a un presupuesto cerrado, no gastar más de lo que uno se puede permitir, no endeudarse para adquirir activos y no tratar de revertir las pérdidas con nuevas inversiones, sino utilizarlas como compensación fiscal (Delfabbro *et al.*, 2021). Por otro lado, es importante alertar a los usuarios sobre el riesgo de adicción. Para ello, sería conveniente establecer un control de la publicidad y promoción de criptoactivos similar al del sector del juego. En este sentido, la Comisión Nacional del Mercado de Valores (CNMV), mediante su Circular 1/2022, ya ha establecido un control sobre la publicidad de criptoactivos con la finalidad de proteger al inversor tratando de garantizar la transparencia de su comercialización, advertir de los elevados riesgos que comportan y evitar la publicidad engañosa.

A fin de promover una inversión responsable y ante el peligro que supone el exceso de información falsa o engañosa en internet, resulta conveniente promover la educación financiera en diversos ámbitos de la sociedad, a través de escuelas, universidades, empresas, entidades del tercer sector o instituciones públicas. Entendemos que es preciso transmitir no solo el conocimiento técnico (tecnológico, financiero y económico) necesario para comprender el funcionamiento de las criptomonedas, sino también una educación que advierta de los riesgos económicos y de adicción que pueden comportar este tipo de instrumentos financieros, además de fomentar una inversión ética y comprometida con la justicia y el bien común de la sociedad, alejada de prácticas puramente especulativas.

**A fin de promover una inversión responsable y ante el peligro que supone el exceso de información falsa o engañosa en internet, resulta conveniente promover la educación financiera en diversos ámbitos de la sociedad [...].**

## Regulación, control y supervisión. Protección del inversor

Durante estos años, el mercado de las criptomonedas ha carecido de regulación nacional e internacional, por lo que se ha convertido en una especie de salvaje Oeste donde cada nuevo criptoactivo establece sus propias normas y protocolos, que, en ocasiones, llegan a burlar la regulación aplicable a instituciones y mercados financieros. Consideramos necesario desarrollar una regulación del mundo de las criptomonedas que tenga en cuenta sus particularidades y que permita establecer un control y una supervisión a los distintos actores implicados. De esta manera, será posible alejar riesgos de contagio al sistema bancario y financiero, proteger al inversor y establecer mecanismos de control para la prevención de delitos.

**[...] muchos Ejecutivos y bancos centrales avanzan hacia una mayor regulación y control de los mercados y servicios de criptomonedas, aunque de forma muy heterogénea.**

En este sentido, muchos Ejecutivos y bancos centrales avanzan hacia una mayor regulación y control de los mercados y servicios de criptomonedas, aunque de forma muy heterogénea. Algunos países han prohibido cualquier actividad relacionada con las criptomonedas, como Egipto, Irak, Qatar, Omán, Marruecos o China. Esta última prohibición en el gigante asiático, en mayo del 2021, causó una importante caída del valor del bitcóin y otras criptomonedas. Rusia ha optado por intervenir y regular este mercado, sobre todo para intentar escapar de las sanciones occidentales como consecuencia de la guerra con Ucrania. En Estados Unidos, aunque los criptoactivos se encuentran sometidos a la normativa sobre mercancías, esta es una regulación bastante laxa. En total, más de 40 países están estudiando formas de regular y supervisar el mercado de las criptomonedas (Otero y Oliver, 2022).

**Europa, por su parte, está elaborando un reglamento sobre los mercados de criptoactivos [...] se incluye legislar sobre los activos digitales y sus intermediarios y proveedores de servicios [...].**

Europa, por su parte, está elaborando un reglamento sobre los mercados de criptoactivos (propuesta MiCA — Market in Crypto Assets—). Entre sus objetivos se incluye legislar sobre los activos digitales y sus intermediarios y proveedores de servicios que no se encuentran sometidos a la normativa vigente en materia de servicios financieros. De esta manera, será posible proveer la necesaria seguridad jurídica y la adecuada protección de los usuarios de criptomonedas (Banco de España, 2022). La propuesta se centra especialmente en el control de aquellos activos como las *stablecoins* que, por su particular relación con divisas nacionales o con otros activos de inversión, pueden comportar serios riesgos de contagio. También se ocupa de establecer mecanismos de protección a los usuarios. Es decir, el objeto principal es la emisión de los *utility tokens* y de los *tokens* de pago que van referenciados a una divisa nacional de curso legal (*stablecoins*); pero quedan fuera de la regulación propuesta el sector de las finanzas descentralizadas (estructuras financieras que utilizan la tecnología *blockchain* pero que replican la lógica de las finanzas tradicionales), lo relativo a la emisión de los *security tokens* (en la medida en que ya se les aplica la normativa MiFID —Markets in Financial Instruments Directive— sobre los mercados e instrumentos financieros), la emisión de los *tokens* no fungibles (como el arte digital) y la emisión de aquellas criptomonedas de pago que no se referencian a ninguna otra moneda de curso legal. Por tanto, el bitcóin y otras criptomonedas puramente especulativas, pese a representar más del 80% del peso de los activos digitales, quedan fuera del marco normativo europeo en lo que atañe a su emisión. Ahora bien, en todos estos casos, si bien la emisión de criptoactivos no se vería afectada por esta normativa, la propuesta sí que regula el control relativo a la prestación de servicios por parte de intermediarios (Banco de España, 2022; PwC, 2021).

En el plano nacional, España no ha desarrollado una normativa específica propia. Tanto el Banco de España como la CNMV han publicado estudios, informes y análisis sobre el mercado de los criptoactivos. Sin embargo, por ahora no disponen de competencias para supervisar o controlar a los intermediarios y prestadores de servicios del mercado de las criptomonedas, aunque se encuentra en proceso de revisión la Ley del Mercado de Valores (del 2015) con la finalidad de dotar a la CNMV de competencias para supervisar los *utility tokens* y otros criptoactivos y otorgar competencias al Banco de España para controlar las *stablecoins*. Este último tan solo es responsable de operar el registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. En el 2021, el Banco de España y la CNMV emitieron un comunicado conjunto en el que advertían de los riesgos de invertir en criptomonedas. A principios del 2022, la CNMV, en el ejercicio de sus competencias, dictó una circular que regula la publicidad de campañas sobre criptoactivos, con la finalidad de que esta se ajuste a contenidos veraces, comprensibles y no engañosos e incluya de forma visible los riesgos asociados a estos activos. En todo caso, ambas instituciones han recomendado el desarrollo de una legislación general sobre criptoactivos (Banco de España, CNMV y DG de Seguros, 2022 Banco de España, 2022.

## Reducir el impacto medioambiental

También consideramos imprescindible introducir cambios para que el uso de criptomonedas sea respetuoso con el medioambiente y no comporte un desmesurado consumo de energía. Al respecto, existen mecanismos de consenso alternativos a la prueba de trabajo que consumen mucha menos electricidad, evitando así el derroche de energía. De hecho, muchos criptoactivos han optado por establecer la denominada *prueba de participación (proof of stake)*. Este sistema de consenso no requiere del uso de la fuerza bruta computacional. La validación está ligada al porcentaje de participación en la red; es decir, será efectuada por el minero que posea un mayor porcentaje de activos de la criptomoneda en cuestión. Los mineros que tienen más participación suelen ser aquellos con más recursos económicos. Por tanto, igual que con la prueba de trabajo, los usuarios con más recursos tienen más probabilidades de obtener la validación, pero las barreras de entrada son menores y además se reduce de forma drástica el consumo de electricidad. Asimismo, al no requerirse dar solución a un problema computacional que implica tiempo, permite un mayor número de validaciones por segundo. Algunas criptomonedas, como polygon, tezos, polkadot y EOS ya han adoptado este tipo de mecanismo consensual; pero el proyecto con mayor impacto seguramente sea la implementación de Etherum 2.0, un nuevo modelo de la criptomoneda etherum basado en la prueba de participación. Además, existirían otros mecanismos alternativos a la prueba de trabajo, como la prueba de historia, que efectúa la verificación a través de la medición del orden temporal exacto sin necesidad de un consumo elevado de energía (Dolader *et al.*, 2017; Kaplan, 2021; Otero y Oliver, 2022).

**[...] muchos criptoactivos han optado por establecer la denominada *prueba de participación (proof of stake)*. Este sistema de consenso no requiere del uso de la fuerza bruta computacional. La validación está ligada al porcentaje de participación en la red [...].**

## La *blockchain* en el sistema financiero tradicional: las finanzas descentralizadas (DeFi)

Aunque ya se ha expuesto que la mayoría de las criptomonedas no son realmente monedas —no pueden ejercer sus funciones básicas y además comportan riesgos importantes— la tecnología subyacente ofrece grandes ventajas y puede ser utilizada para ganar eficiencia en campos muy diversos, entre ellos el de las finanzas tradicionales. En este sentido, el BPI señaló que la tecnología *blockchain* y su red descentralizada podía servir para hacer más eficiente el servicio de pagos internacionales de divisas nacionales, en el que el coste del múltiple registro de los bloques de *blockchain* es inferior al de la opción centralizada de sucesivos intermediarios. En este sentido, algunas entidades financieras han desarrollado criptomonedas de forma específica para la utilización de determinados servicios financieros. Esta ventaja se utilizó, por ejemplo, en la gestión de pagos internacionales benéficos para ayuda a los refugiados de Siria en Jordania. También se puede aprovechar esta tecnología para combinar un sistema de pagos descentralizado de monedas nacionales con la ejecución de contratos inteligentes a través de sofisticados códigos programados en los activos. En todos estos casos, se estaría utilizando la tecnología que soporta las criptomonedas para mejorar el sistema de pagos o las finanzas basadas en monedas fíat (BPI, 2018).

**[...] el BPI señaló que la tecnología *blockchain* y su red descentralizada podía servir para hacer más eficiente el servicio de pagos internacionales de divisas nacionales [...].**

Muchas entidades financieras están investigando y trabajando para incorporar la tecnología *blockchain* a sus servicios de finanzas tradicionales. Por ejemplo, CaixaBank ya lanzó en el 2020 la plataforma we.trade para ejecutar y financiar transacciones de comercio exterior a sus clientes de empresa a través de la tecnología *blockchain*, lo que la convirtió en una de las primeras entidades de toda Europa en ofrecer un servicio de estas características (CaixaBank, 2020). El Banco Santander también lanzó en el 2019 su primer bono completamente digital utilizando la red *blockchain* de Ethereum (Otero y Oliver, 2022).

## Criptomonedas emitidas por bancos centrales

Probablemente las denominadas *stablecoins* son los criptoactivos que se han tomado más en serio la búsqueda de un ancla que pueda estabilizar su valor para tratar de sustituir a las monedas fíat, al referenciar su valor nominal al de diferentes monedas soberanas. Ahora bien, como ya hemos sugerido con anterioridad, han tenido importantes problemas y no han logrado tampoco erigirse como auténticas monedas digitales, además de necesitar la confianza que generan las monedas emitidas por los bancos centrales. Por otro lado, aunque la utilización de la tecnología *blockchain* en las finanzas tradicionales puede servir para alcanzar una mayor eficiencia en dicho sector sin arrastrar los elevados riesgos de las criptomonedas, el BPI lo ve como un pequeño parche que no soluciona el problema de forma adecuada, pues solo se puede aplicar a una pequeña parte de las finanzas y se trata de un sistema centralizado que no dispone de una regulación adecuada (BPI, 2022).

**[...] sugiere que el futuro de las divisas digitales se encuentra en las monedas digitales emitidas por bancos centrales (MDBC) [...].**

Por ello, sugiere que el futuro de las divisas digitales se encuentra en las monedas digitales emitidas por bancos centrales (MDBC) —en inglés, *central bank digital currencies*, CBDC—, al ser estas autoridades los únicos intermediarios capaces de generar la adecuada confianza, posibilitar que las monedas sirvan como unidad de cuenta, asegurar la adecuada liquidez o salvaguardar la integridad del sistema de pagos a través de regulación, control y supervisión. Según el BPI, la utilización de la tecnología *blockchain* podría servir para ofrecer la programabilidad de los contratos inteligentes, permitir transacciones entre una mayor variedad de intermediarios (además de las entidades financieras) o mejorar la eficiencia de los pagos internacionales. A través de la "tokenización" de los depósitos de dinero se podría optimizar la interoperabilidad entre los clientes y las plataformas o permitir la instantaneidad de los pagos (BPI, 2022).

Un estudio publicado por CaixaBank Research (García y Guasch, 2018) ya sugería en el 2018 los beneficios de una criptomoneda emitida por bancos centrales, al disponer la autoridad central de los adecuados mecanismos institucionales en el sistema financiero, de la competencia para emitir dinero de curso legal, de credibilidad y confianza y de capacidad de control y supervisión.

En el 2020, el Banco de España publicó un estudio (Ayuso y Conesa, 2020) sobre la creación de monedas digitales emitidas por bancos centrales, en el que se señalaba la posibilidad de emitir una moneda digital similar al efectivo para reducir la dependencia del sector privado o de empresas extranjeras, para fomentar la inclusión financiera al reducir costes y aumentar en seguridad o para diseñar un sistema de pagos más eficiente.

**[...] la emisión de monedas digitales emitidas, controladas y respaldadas por bancos centrales podría reducir muchos de los riesgos éticos que comportan las criptomonedas, en especial, su carácter especulativo o su condición de vehículo para la comisión de delitos.**

A día de hoy, ya se han emitido tres proyectos de monedas digitales respaldadas por bancos centrales (Bahamas, Nigeria y Organización de Estados del Caribe Oriental). China, después de prohibir cualquier actividad relacionada con las criptomonedas, también está considerando la posibilidad de emitir una moneda digital respaldada por su autoridad central. Estados Unidos, el Reino Unido o Rusia también están realizando estudios. Por su parte, el Banco Central Europeo (BCE) está investigando desde el año 2020 la puesta en marcha del euro digital, aunque el proyecto aún se encuentra en una fase muy incipiente (Otero y Oliver, 2022).

En todo caso, la emisión de monedas digitales emitidas, controladas y respaldadas por bancos centrales podría reducir muchos de los riesgos éticos que comportan las criptomonedas, en especial, su carácter especulativo o su condición de vehículo para la comisión de delitos.

# 5. CONCLUSIONES

La aparición de las criptomonedas se enmarca en un proceso de digitalización de la sociedad y ha comportado grandes innovaciones tecnológicas en el campo de la prestación de servicios de pago. Su origen también se encuentra marcado por el colapso del sistema financiero en la crisis del 2008. Por eso, no es de extrañar que el diseño de las criptomonedas pretendiera construir un modelo transgresor de moneda digital, que se erigiera como alternativa al dinero fiduciario y al sistema financiero tradicional. El funcionamiento de las criptomonedas prescinde de los Gobiernos, de los bancos centrales y de las entidades financieras y presume de una gobernanza democrática, transparente y descentralizada en la que los usuarios se relacionan en un plano de igualdad.

**[...] el mercado de las criptomonedas y la tecnología que las soporta ha dejado al descubierto una serie de riesgos éticos que, como sociedad, debemos afrontar.**

Ahora bien, ya hemos observado que las criptomonedas no han conseguido sustituir al dinero fiduciario de los Estados soberanos, ya que, en la mayoría de los casos, no pueden ejercer las tres funciones básicas del dinero: ser unidad de cuenta, medio de cambio y depósito de valor. La mayoría de las criptomonedas tienen una elevada volatilidad causada por la especulación y las *stablecoins*, aun manteniendo cierta estabilidad, han tenido también importantes problemas. La gobernanza descentralizada de los criptoactivos (sin intermediarios ni autoridad central) ha fracasado a la hora de generar confianza en la sociedad. No han conseguido cumplir con el requisito de aceptación universal, imprescindible para el funcionamiento de cualquier divisa.

Pero, además, el mercado de las criptomonedas y la tecnología que las soporta ha dejado al descubierto una serie de riesgos éticos que, como sociedad, debemos afrontar. La mayoría de las transacciones de criptomonedas se deben exclusivamente a la especulación y algunos autores atribuyen este carácter especulativo a la propia naturaleza y el funcionamiento de los criptoactivos. La pseudoanonimidad que requiere la transparencia de la red ha permitido que las criptomonedas se conviertan en un instrumento para la comisión de delitos o la financiación de terrorismo, mafias y guerras. La ausencia de regulación deja sin protección al inversor. El carácter especulativo ha fomentado los problemas de adicción, especialmente entre los más jóvenes. Por último, la propia tecnología *blockchain* y, en especial, algunos mecanismos de consenso, requieren un desmesurado consumo de energía, lo cual acarrea un impacto negativo para el medioambiente.

Aunque los problemas que afectan el campo de la ética son serios e importantes, no deberían desaprovecharse los beneficios, las oportunidades y las innovaciones tecnológicas que han traído las criptomonedas y la tecnología *blockchain*. Por ello, en este cuaderno se tratan estos retos éticos y se proponen una serie de recomendaciones que pueden paliar sus consecuencias negativas y ayudar a diseñar un modelo de monedas digitales ético y sostenible:

**Aunque los problemas que afectan el campo de la ética son serios e importantes, no deberían desaprovecharse los beneficios, las oportunidades y las innovaciones tecnológicas [...].**

- Promover, a través de la educación financiera, un modelo de inversión responsable alejado de la especulación y que disponga de mecanismos para luchar contra los problemas de adicción.
- Establecer regulaciones nacionales y supranacionales que permitan prevenir la comisión de delitos o la financiación de actividades ilícitas, alejar al sistema financiero de riesgos sistémicos, supervisar a los intermediarios (especialmente en una red descentralizada) y proteger al inversor.

- Reducir el impacto medioambiental de la tecnología *blockchain* a través de mecanismos de consenso que no requieran fuerza bruta computacional.
- Utilizar la tecnología *blockchain* y el desarrollo de criptoactivos en aquellos casos en que pueda mejorar y hacer más eficiente el sistema de finanzas tradicionales.
- Estudiar y desarrollar monedas digitales emitidas por bancos centrales que puedan beneficiarse de las ventajas de la digitalización y, al mismo tiempo, generar confianza, alejarse de la especulación y desarrollar medidas de seguridad y prevención de delitos. Todo ello, a través de una autoridad central pública que pueda desarrollar una política monetaria al servicio de la sociedad.

La complejidad de las criptomonedas requiere de un debate transversal y multidisciplinar. Todas estas recomendaciones pretenden contribuir desde el campo de la ética y aportar una reflexión necesaria para la construcción de un modelo de monedas digitales que tenga en cuenta la auténtica finalidad del dinero, es decir, servir como un instrumento para que las personas puedan adquirir a través del comercio los bienes y servicios necesarios para su desarrollo, con respeto a su dignidad y con el objetivo de lograr el bien común de la sociedad.

# BIBLIOGRAFÍA

ARNAL, J., MENÉNDEZ-MORÁN, M. E. Y MUÑOZ J. (2021). *Quo vadis, Bitcoin?* Real Instituto Elcano. https://www.realinstitutoelcano.org/en/analyses/quo-vadis-bitcoin/

ARNER, D., AUER, R. Y FROST, J. (2020). Stablecoins: Risks, potential and regulation. *BIS Working Papers, n.º 905*. Bank for International Settlements. https://www.bis.org/publ/work905.pdf

AUER, R. Y TERCERO-LUCAS, D. (2021). Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments. *BIS Working Papers, n.º 951*. Bank for International Settlements. https://www.bis.org/publ/work951.pdf

AYUSO, J. Y CONESA, C. (2020). Una introducción al debate actual sobre la moneda digital de banco central (CBDC). *Documentos Ocasionales, n.º 2005.* Banco de España. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/20/Fich/do2005.pdf

BAGUS, P. Y DE LA HORRA, P. L. (2021). An ethical defense of cryptocurrencies. *Business Ethics, the Environment & Responsibility, vol. 30(5)* (pp. 423-431). https://doi.org/10.1111/beer.12344

BANCO DE ESPAÑA. (2022). Especial criptoactivos. *Informe de Estabilidad Financiera* (pp. 149-175). https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinancera/22/IEF_2022_1_CapE.pdf

BANCO DE ESPAÑA, CNMV Y DG DE SEGUROS. (2022). Comunicado conjunto del Banco de España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos. https://www.cnmv.es/Portal/verDoc.axd?t=%7B17510971-c6cb-4b94-95d6-509b4061598f%7D

BANCO DE PAGOS INTERNACIONALES. (2018). Cryptocurrencies: looking beyond the hype. *BIS Annual Economic Report* (pp. 91-114). https://www.bis.org/publ/arpdf/ar2018e5.pdf

BANCO DE PAGOS INTERNACIONALES. (2022). The future monetary system. *BIS Annual Economic Report* (pp. 75-115). https://www.bis.org/publ/arpdf/ar2022e3.pdf

BERENTSEN, A. Y SCHAR, F. (2018). A short introduction to the world of cryptocurrencies. *Federal Reserve Bank of St. Louis, Review, vol. 100(1)* (pp. 1-16). https://doi.org/10.20955/r.2018.1-16

BTCDIRECT. (s. f.). *Precio de Bitcoin.* BTCdirect.eu. https://btcdirect.eu/es-es/precio-bitcoin

CAIXABANK. (3 de enero del 2020). *CaixaBank lanza la plataforma "blockchain" we.trade para ejecutar y financiar transacciones de comercio exterior de sus clientes de empresa* [Nota de prensa]. https://www.caixabank.com/comunicacion/noticia/caixabank-lanza-la-plataforma-*blockchain*-we-trade-para-ejecutar-y-financiar-transacciones-de-comercio-exterior-de-sus-clientes-empresa_es.html?id=42117

COINMARKETCAP. (s. f.). [Página web de seguimiento de precios de criptomonedas]. CoinMarketCap.com. https://coinmarketcap.com

CONESA, C. (2019). Bitcoin: ¿una solución para los sistemas de pago o una solución en busca de problema? *Documentos Ocasionales, n.º 1901.* Banco de España. https://repositorio.bde.es/bitstream/123456789/8803/1/do1901.pdf

CONKLIN, M. Y CEBALLOS, R. (2022). The ethics of investing in cryptocurrencies. *FLA ST. BUS. REV. 69.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3919795

DELFABBRO, P., KING, D., WILLIAMS, J. Y GEORGIOU, N. (2021). Cryptocurrency trading, gambling and problem gambling. *Addictive Behaviors, vol. 122.* https://doi.org/10.1016/j.addbeh.2021.107021

DOLADER, C., BEL, J. Y MUÑOZ, J. L. (2017). La *blockchain*: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial, n.º 405* (pp. 33-40). https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf

EUROPOL (2021). Cryptocurrencies: Tracing the evolution of criminal finances. *Europol Spotlight Report series, Publications Office of the European Union.* https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

FERNÁNDEZ, E. (15 de enero del 2018). *La fiebre de las criptomonedas.* CaixaBank Research. https://www.caixabankresearch.com/es/economia-y-mercados/mercados-financieros/fiebre-criptomonedas.

FOLEY, S., KARLSEN, J. Y PUTNIŅŠ, T. (2019). Sex, drugs, and bitcoin: How much illegal activity is finances through *cryptocurrencies? The Review of Financial Studies, vol. 32(5)* (pp. 1798-1853). https://doi.org/10.1093/rfs/hhz015

GARCÍA, J. Y GUASCH, M. (15 de mayo del 2018). *El dinero digital en la economía del futuro: nuevas posibilidades, nuevos retos.* CaixaBank Research. https://www.caixabankresearch.com/es/analisis-sectorial/banca/dinero-digital-economia-del-futuro-nuevas-posibilidades-nuevos-retos

GSCHOSSMANN, I., VAN DER KRAAIJ, A., BENOIT, P. L. Y ROCHER, E. (2022). Mining the environment – is climate risk priced into crypto-assets? *European Central Bank, Macroprudential Bulletin, n.º 18.* https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_3~d9614ea8e6.en.html

HOUBEN, R. Y SNYERS, A. (2018). Cryptocurrencies and *blockchain*. Legal context and implications for financial crime, money laundering and tax evasion. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf

KAPLAN, E. (25 de mayo del 2021). *Cryptocurrency goes green: Could 'proof of stake' offer a solution to energy concerns?* NBC News. https://www.nbcnews.com/tech/tech-news/cryptocurrency-goes-green-proof-stake-offer-solution-energy-concerns-rcna1030

MAKAROV, I. Y SCHOAR, A. (2021). *Blockchain Analysis of the Bitcoin Market.* SSRN. http://dx.doi.org/10.2139/ssrn.3942181

NAKAMOTO, S. (2008, October 31). Bitcoin P2P E-cash paper. Welcome page. https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

NIETO, M. A. Y HERNÁEZ, J. (2018). Monedas virtuales y locales: las paramonedas, ¿nuevas formas de dinero? *Revista de estabilidad financiera, n.º 35* (pp. 103-122). Banco de España. https://repositorio.bde.es/bitstream/123456789/11245/1/Monedas_virtuales_y_locales_las_paramonedas.pdf

O'NEILL, J. (18 de marzo del 2021). La lotería del bitcoin. *Política Exterior.* https://www.politicaexterior.com/la-loteria-del-bitcoin/

OSSA, F. (1992). Dinero y sistemas monetarios alternativos. *Pontificia Universidad Católica de Chile, Cuadernos de Economía, vol. 29(86)* (pp. 1-34). https://www.econbiz.de/Record/dinero-y-sistemas-monetarios-alternativos-ossa-scaglia-fernando/10001122314

OTERO, M. Y OLIVER, P. (2022). Criptomonedas, *stablecoins* y la criptoeconomía: el estado de la cuestión [Documento de Trabajo 2/2022]. Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2022/04/dt-2022-otero-oliver-criptomonedas-stablecoins-y-la-cripto-economia-el-estado-de-la-cuestion-1.pdf

PORRAS, E. Y DAUGHERTY, B. (2021). Bitcoin and ethics in a technological society. En T. M. Fernández-Caramés y P. Fraga-Lamas (eds.), *Advances in the Convergence of Blockchain and Artificial Intelligence.* IntechOpen. https://doi.org/10.5772/intechopen.96798

PWC. (2021). *El impacto regulatorio de la Propuesta MiCA.* PwC.es. https://www.pwc.es/es/auditoria/assets/impacto-regulatorio-mica-en%20los-criptoactivos.pdf

RAMÍREZ, N. (26 de junio del 2022). *Varios menores vinculados a criptoestafas, en paradero desconocido.* RTVE.es. https://www.rtve.es/noticias/20220626/varios-menores-vinculados-criptoestafas-paradero-desconocido/2367283.shtml

ROMERO, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Economic Bulletin 4/2018. Analytical Articles.* Banco de España. https://repositorio.bde.es/bitstream/123456789/8985/1/beaa1804-art26e.pdf

RODRIGUEZ, D. (2022). Los psicólogos de la Comunitat alertan de que los jóvenes han sustituido la adicción a las apuestas deportivas por la especulación con criptomonedas. Cadena Ser. https://cadenaser.com/2022/04/30/los-psicologos-de-la-comunitat-alertan-de-que-los-jovenes-han-sustituido-la-adiccion-a-las-apuestas-deportivas-por-la-especulacion-con-criptomonedas/

RTVE. (8 de abril del 2022). *Badalona acoge un congreso de formación financiera y criptomonedas bajo acusaciones de estafa piramidal.* RTVE.es. https://www.rtve.es/noticias/20220408/badalona-acoge-congreso-formacion-financiera-bajo-acusaciones-estafa-piramidal/2329560.shtml

SANDEL, M. (2013). *The moral economy of speculation: Gambling, finance, and the common good. En Tanner Lectures on Human Values* (pp. 333-359). University of Utah. https://tannerlectures.utah.edu/_resources/documents/a-to-z/s/Sandel%20Lecture.pdf¡

SERRANO, A. (20 de noviembre del 2021). El alto riesgo que corren los jóvenes con su adicción a las criptomonedas. *El Economista*. https://www.eleconomista.es/actualidad/noticias/11458821/10/21/El-alto-riesgo-que-corren-los-jovenes-con-su-adiccion-a-las-criptomonedas.html

TECNOPASION.NET (2022). Entrevista con el Dr. Jeremiah Weinstock, Universidad de Saint Louis, sobre la adicción al comercio de criptomonedas. https://www.tecnopasion.net/entrevista-con-el-dr-jeremiah-weinstock-universidad-de-saint-louis-sobre-la-adiccion-al-comercio-de-criptomonedas/

VALENZUELA, S. (s. f.). *Bitcoin y Lightning Network.* Sergiovalezuela.es. https://sergiovalenzuela.es/tips-basicos-sobre-bitcoin-y-lightning-network/

VERMA, P. (29 de abril del 2022). Insomnia, addiction, depression: The dark side of life trading crypto. *The Washington Post.* https://www.washingtonpost.com/technology/2022/04/29/crypto-addiction/

www.iese.edu

Barcelona
Madrid
Munich
New York
São Paulo

IESE Business School
University of Navarra

Cátedra CaixaBank
de Sostenibilidad
e Impacto Social

**A Way to Learn. A Mark to Make. A World to Change.**