# CRIPTOACTIVOS, BLOCKCHAIN Y NFT´S

SAMUEL CRUZ PALENZUELA
**Decano COTIME Tenerife**
**UNIVERSIDAD EUROPEA DE CANARIAS**

El presente artículo realiza un descriptor de análisis de las criptomonedas en su conjunto, para definir su realidad tecnológica, su finalidad e idoneidad, y sin ser un asesoramiento al efecto, centra este recorrido en una introducción interpretativa al mundo de las criptomonedas desde los conceptos clave, entendiendo las principales ventajas y desventajas de estas, la relación con la verificación compuesta de blockchain y la apertura a procesos complejos basados en los NFT´s (non fungible tokens) y, por último, realizando un elenco de las distintas criptomonedas que ofrece el mercado.

**PALABRAS CLAVE •**
Criptomonedas, NFT´s, criptoactivos, tokens, blockchain

**CÓMO CITAR ESTE ARTÍCULO •**
Cruz Palenzuela, Samuel. 2022, "**Criptoactivos, Blockchain y NFT´s**" en: UEM STEAM Essentials

## INTRODUCCIÓN

Las *criptomonedas* o *monedas digitales encriptadas*, pueden no ser "tan grandes como una imprenta" según sus defensores, pero su actual desarrollo ha dejado una enorme herramienta de influencia: la tecnología *blockchain* como una estructura de datos pública (Figuero Castilla, 2020).

Hay más de 10,000 monedas digitales en la actualidad[1] de las cuales *Bitcoin* se destaca actualmente como la criptomoneda preeminente, nacida en 2008 y hecha pública en 2009. Algunos de sus pilares y aspiraciones fundamentales, basados en protocolos y software que se inspiraron hace décadas en el manifiesto de 1992 de Timothy C. May para el *criptoanarquismo*. El *criptoanarquismo* es una ideología estratégica que favorece el uso de la criptografía asimétrica para hacer cumplir los principios de privacidad y libertad personal.

El término fue popularizado por Timothy C. May[2] y descrito por Vernor Vinge como la encarnación del anarcocapitalismo en el ciberespacio. El objetivo de los criptoanarquistas es crear software encriptado para evadir el enjuiciamiento y el acoso mediante el envío y la recepción de información a través de redes informáticas.

Su predicción se ha hecho realidad en cierto modo, y aunque queda por ver si tendrá un impacto similar al de la imprenta, *bitcoin* toma la idea de este manifiesto criptoanarquista y le da vida a través de un sistema de tecnología *blockchain* (figura 1). Los críticos lo ven como una burbuja, mientras que sus defensores advierten sobre una revolución tecnológica que se avecina. Lo cierto es que la irrupción de Bitcoin ha dado lugar a otras criptomonedas que incluso se disputan cuota de mercado. Queda por ver en

**1 »** Actualmente existen más de 17.000 criptomonedas distintas a fecha de Febrero 2022. Muchas de estas criptomonedas tienen poco o ningún volumen de negociación, pero por el contrario muchas otras cuentan con un gran número de inversores y de comunidades dedicadas a su desarrollo. Fuente: Guía de trading Enero 2022.

**2 »** Timothy C. May, fallecido en 2018, escribía en 1992 el considerado el tratado fundacional del criptoanarquismo: Cyphernomicon. Disponible en https://www.oroyfinanzas.com/2014/04/manifiesto-cripto-anarquista-timothy-c-may-1992-cryptoanarchist-manifesto/

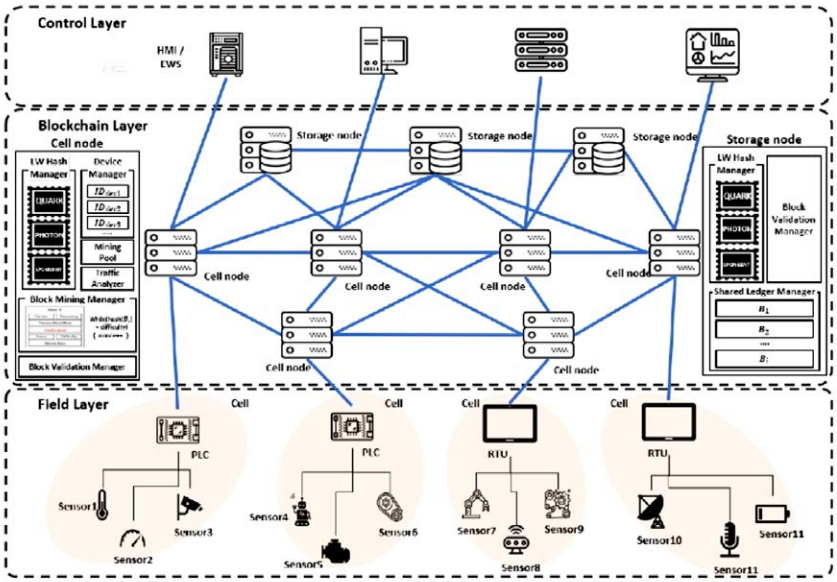


**Figura 1 »** Arquitectura de blockchain en aplicación para Internet of Things, IoT. (Fuente: Seok, Park y Hyuk 2019)

qué medida el capital financiero puede contener o adaptarse a este fenómeno.

Más allá del futuro de *bitcoin*, el advenimiento de la tecnología *blockchain*[3] abre la posibilidad de cambiar cualquier práctica social que deba proteger la identidad y autenticidad de los documentos. Sus posibles aplicaciones son el tema más candente en la comunidad de programadores, quienes prometen que en menos de cinco años transformará la mayoría de las áreas de la vida cotidiana, como los pasaportes, el almacenamiento masivo en línea e incluso el proceso electoral.

## ¿QUÉ SON LAS CRIPTOMONEDAS?

Las criptomonedas son monedas digitales basadas en una serie de fórmulas matemáticas muy avanzadas, descentralizadas y anónimas. Cuando se trata de monedas descentralizadas, se refiere a criptomonedas que no requieren una autoridad central para protegerlas y controlarlas (Silva, 2018). Esto es diferente de lo que sucedería con las monedas fiduciarias, que se conocen hoy, por ejemplo, dependiendo del euro en el Banco Central Europeo o del dólar en la Reserva Federal.

Creadas por Satoshi Nakamoto, del cual se desconoce si es un individuo o un alias para un grupo de trabajo (Lemieux 2013) este trató de dibujar un nuevo sistema entre pagos electrónicos directos y similares mediante el uso de *blockchain*, a través de la moneda estrella bitcoin. A estas transacciones de pago se denominan sistemas *peer-to-peer* o *P2P* (Pacheco, 2020).

El estudio de estas transacciones P2P se caracterizan porque no es necesario que un tercero la manipule y se establecen una serie de reglas plasmadas en forma de computación distribuida para asegurar la integridad de la transacción, todo ello mediante la aplicabilidad de la *blockchain* (Almonacid Sierra, 2020). Las criptomonedas se utilizan y aceptan como medio de pago siempre que las partes así lo acuerden, y como tal, se utilizan como cualquier otra moneda que se puede cambiar por bienes y servicios. El hito que ha logrado Satoshi Nakamoto no es la creación de una moneda digital, ya que antes han existido otras monedas digitales, como *Digicash*, en muchos términos fallida (Gamage, 2020). El éxito estará en no depender de un tercero para intercambiarlas.

La inspiración de Satoshi Nakamoto no solo se basó en la aplicación de algoritmos, sino también en la experiencia de diferentes corrientes de pensamiento de la época, conocidas como *Cypherpunk* (Swartz, 2018). Satoshi Nakamoto tuvo que enfrentar y superar diferentes desafíos combinados con seis aspectos fundamentales para poder olvidarse de los problemas criptográficos y los complejos sistemas de red que hacen posibles las monedas digitales descentralizadas.

## RETOS Y PROBLEMAS DE LAS CRIPTOMONEDAS

El desafío más relevante para un uso global de las criptomonedas que Satoshi Nakamoto tuvo que superar, tiene que ver con la creación de una cuenta corriente impresa. La creación de la cuenta se realiza a partir de una clave privada generada aleatoriamente y, una vez generada, se aplica un algoritmo para crear la clave pública. Esta clave pública se usa como nuestro número de cuenta bancaria para recibir transacciones y la clave privada se usa como contraseña. El número de claves en la práctica es imposible de descifrar. Ello puede implicar una serie de retos y problemas. Los principales retos a resolver[4] se dividen en:

» a) *Evitar las falsificaciones*

» b) *Evitar prohibiciones gubernamentales*

» c) *Actualizaciones de la base de datos*

» d) *Monitoreo de los mineros de datos*

» e) *Producción de monedas*

» f) *Entrega de cuentas corrientes a los usuarios*

3 » "Blockchain, cadena de bloques en inglés, es un registro digital que está repartido entre varios participantes sin que exista una autoridad central. Puede decirse que es una base de datos de transacciones descentralizada y distribuida entre varios nodos" (del Pozo 2021)

4 » A reseñar los grandes robos de criptomonedas de la historia en relación a estas problemáticas, fundamentalmente de los dos principales problemas: volatilidad y fraude. https://www.euribor.com.es/2021/04/12/las-criptomonedas-problemas/

El **primer reto** es evitar la falsificación de moneda, porque si se copia fácilmente, no tendrá valor, a este se le llama el problema del doble gasto. En lugar de ofrecer monedas a los usuarios, Satoshi Nakamoto creó un libro de contabilidad que muestra cuántas monedas posee cada usuario. Sin moneda, no se puede replicar, por lo que el uso de claves privadas y contraseñas permite a cada usuario realizar transacciones a través de entradas en todos los libros de contabilidad de la cadena de bloques.

El **segundo reto** busca evitar prohibiciones gubernamentales. Los libros de contabilidad digital en sí no son nuevos, por ejemplo, *paypal* los usa. Sin embargo, estos dependen de un tercero. Para superar esto, Satoshi replicó el sistema utilizado por *bittorrent*, un software que permite descargar películas y música a través de porciones aportadas por las diferentes computadoras de cada usuario, de modo que cuando alguien quiere descargar una película en particular, la descarga se realiza a través de la red de miles de computadoras.

El **tercer reto** trata de solucionar el problema de la actualización de la base de datos. Queriendo un sistema descentralizado que no dependiera de terceros, Satoshi Nakamoto creó un sistema a través del cual ciertas computadoras llamadas mineros se encargaban de actualizar el libro mayor y obtenían mediante la prueba de trabajo (denominada *proof of work* en inglés) una recompensa. Para actualizar el libro mayor, estos mineros de datos[5] necesitan una prueba de trabajo que resuelva un problema matemático que implica encontrar un número más pequeño que el número objetivo mediante una función criptográfica que genera números aleatorios.

Este sistema se llama *hashing*. Cada vez que los mineros resuelven el sistema, recolectan recompensas y pueden modificar una base de datos que será verificada por el resto de la red, y si hacen entradas fraudulentas o mal escritas, pierden las recompensas que ganan. De esta manera, los mineros siempre actuarán con honestidad y evitarán que el sistema se vea comprometido. En pocas palabras, al construir la red Bitcoin de esta manera, es casi imposible de piratear, lo que la convierte en la red más segura del mundo.

El **cuarto reto** es la necesidad de monitorear a los mineros, y Satoshi Nakamoto creó nodos que actúan como guardianes del sistema para evitar infracciones dentro de ellos.

El **quinto reto** está relacionado con la producción de monedas, *bitcoin* está limitado a 21 millones de unidades[6] , número que se alcanzará en el año 2140, además, se sabe que cada 4 años la producción de *bitcoin* se reduce a la mitad, fenómeno conocido como *halving*. Por lo tanto, los precios y las demandas pueden variar, pero las ofertas no. Los precios y demandas de los criptoactivos pueden variar, pero la oferta no, ya que está limitada en número y tiempo.

Dado que la demanda de *bitcoin* no puede cambiar porque siempre se sabe cuánta moneda hay en circulación, un aumento en la demanda hace que el precio suba, lo que a su vez provoca la volatilidad del valor de la moneda (figura 2).

Además de estos retos, existe otro riesgo potencial debido a que el manejo de las criptomonedas también puede dar lugar a la posibilidad de esquemas piramidales o esquemas *Ponzi*. Como ya hemos visto a lo largo de la exposición, las criptomonedas son activos con un gran potencial, no solo monedas convertibles, también representan un objeto de inversión con anonimato y seguridad. Sin embargo, su formato digital y anónimo pueden ser potencialmente peligrosos.[7]

En el mundo de las criptomonedas, un esquema *Ponzi* o esquema piramidal es un sistema que intenta vender una gran cantidad de rentabilidad en un corto período de tiempo, cuando otros usuarios no acceden a ingresar al sistema o al mismo tiempo exigen que se les devuelva su dinero, estos sistemas quebrarían ocasionando pérdidas a todo usuario. Algunos ejemplos de tales estafas son: *Onecoin*, la compañía que creó la moneda del mismo nombre se convirtió en

5 » Término referido a la minería de datos o data mining como proceso de examen de datos ya recogidos, con nuevos algoritmos, para generar nuevas informaciones y/o encontrar patrones.

6 » Sin embargo, la gran mayoría de las monedas (99%) se habrán extraído alrededor de 2032, cuando el subsidio por bloque se reduzca a menos de 1 BTC por bloque. Existirán aproximadamente 20,67 millones de monedas, lo que dejará menos de 1/2 millón para minar en los próximos 100 años. Disponible en https://en.bitcoin.it/wiki/Controlled_supply

7 » Una duda recurrente es ¿qué ocurriría en caso de herencia? ¿se podría perder por no ser recuperable o localizable tras un fallecimiento? la pérdida o robo puede deducirse fiscalmente, siempre y cuando se cumplan los requisitos que tienen que ver con denunciar y demostrar la efectiva pérdida. El fallecimiento implicaría que las cripto deben ser parte de la herencia, al ser un activo más, con un valor.

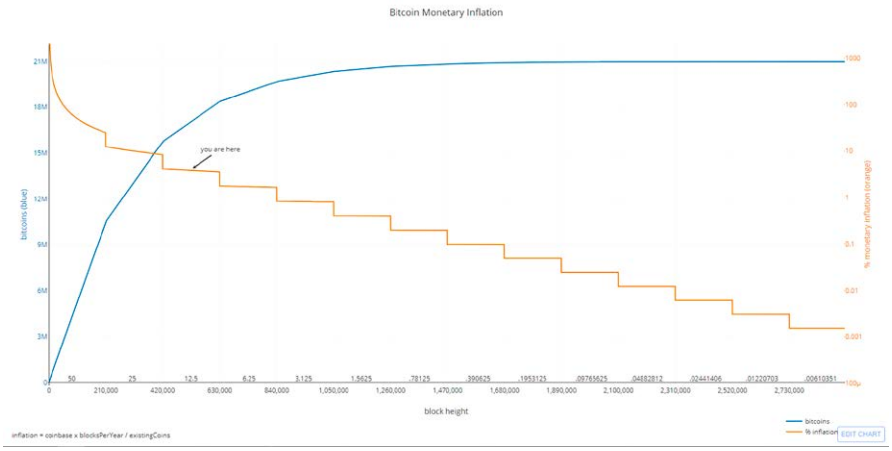


**Figura 2 »** Inflación monetaria del Bitcoin por número de bitcoins totales (fuente: https://chart-studio.plotly.com/~BashCo/5.embed?share_key=IjQ-VkaTiHXjX2W41UiqzCn)

el esquema piramidal más grande conocido en el mundo de las criptomonedas. Otro ejemplo muy conocido es la plataforma *Bitconnect*, que permite a sus usuarios pedir prestado dinero en *bitcoin* por un período determinado, el atractivo de esta plataforma es el beneficio que prometen a través de lo que se llama interés sobre el préstamo. Este caso es especial porque sucedió en un momento muy específico del mercado, de emoción colectiva, inversores sin experiencia y promesas muy atractivas. Sucedió en 2017, y dado que fue un año en que el valor de Bitcoin aumentó, fue una llamada de atención para los usuarios.

Es necesario recordar, al referirse a estos esquemas, nadie va a donar dinero, y los grandes beneficios inculcados por los programas de referencia a menudo acompañan a los esquemas Ponzi.[8]

Un reto añadido más es el coste medioambiental del minado de dato, pues se necesita que los ordenadores estén permanentemente encendidos, lo que masivamente implica un consumo medioambiental muy relevante, del orden de 40 kWh semanales.[9]

## CONCEPTOS CLAVE EN EL MUNDO CRYPTO

Cualquiera que quiera comprar o invertir en una criptomoneda específica debe comprender algunos conceptos básicos para poder operar con seguridad en el mundo de las monedas digitales. Las casas de cambio o *exchange* de criptomonedas es el lugar para comprar estos activos digitales. Dentro de las funciones de estas casas de cambio, está la de proveer liquidez a los usuarios en un ambiente de negocios seguro y organizado. Hay dos tipos de intercambios: centralizados y descentralizados.

Las casas de cambio centralizadas, conocidas por las siglas *CEX*, se asimilan a una entidad bancaria ya que suele ser una empresa privada que actúa como intermediaria y se encarga de ejecutar cualquier tipo de transacción. Podemos realizar transferencias o pagos con tarjeta en dinero fiduciario al propio exchange para comprar nuestra criptomoneda posteriormente. Podemos, a su vez, hacer lo contrario, vendiendo nuestros criptoactivos por moneda fiduciaria. En estos Exchanges, el valor de la moneda lo proporciona el propio mercado de oferta y demanda. Los intercambios más famosos son *Binance*, *Coinbase*, *Kucoin* o *Bit2me*.

Las casas de cambio descentralizadas conocidas por las siglas *DEX* se encargan de eliminar intermediarios y realizar transacciones en un entorno automatizado basado en contratos inteligentes. Los *tokens*[10] más innovadores que no encontraremos en los intercambios centralizados los encontraremos en los *DEX*, donde el precio de las criptomonedas estará determinado por una fórmula matemática llamada *AMM*, siglas de abreviatura de *Automated Market Maker*s. Esta fórmula nunca será la misma y puede variar según el protocolo. El intercambio más famoso es *HodlHodl*.

En ambos casos, tanto de casas CEX como DEX, los precios en ambos son puestos por el mercado, no obstante, las comisiones que se imponen en CEX son más caras que en DEX, de ahí que sea algo más barato. Poniendo un ejemplo práctico, la plataforma *Coinbase* (CEX) cobra una comisión del 0,5% del valor total de transacción, en cambio, los pools de *Uniswap* (DEX) normalmente cobrar un 0,3%.

Principales ventajas CEX: gran volumen de operaciones y gran liquidez, intercambios de cripto a cripto y de cripto a fiat, gran nivel de funcionalidad, fáciles de usar mediante transacciones rápidas.

Desventajas CEX: Alta posibilidad de pirateos y fraudes, escasa regulación gubernamental.

Ventajas DEX: más seguros que CEX, bajos porcentajes de comisión, no sujetos a regulación y no podrían ser cerrados por un Gobierno, ofrecen accesos a variedad de tokens.

Desventajas DEX: Escasa liquidez y funcionalidad limitada.

Una *wallet* es una billetera utilizada para almacenar cualquier moneda. Así que lo primero para poder tener uno de estos es conseguir una billetera digital que sea completamente gratuita y de libre acceso para los usuarios. Además, están disponibles para la mayoría de los dispositivos móviles y ordenadores con diferentes sistemas operativos.

Las billeteras (figura 3) son las encargadas de almacenar las claves públicas y privadas que permiten a los usuarios operar con criptomonedas, en este caso, enviar y recibir criptomonedas, ya su vez, llevan un registro de todas las transacciones realizadas como un libro de contabilidad.

8 » El último caso reciente, en Tenerife, donde una empresa llamada Axxxxxxr prometió grandes beneficios a sus usuarios en el mismo sistema que todos los demás, perdió fondos para muchos inversores, y el caso está actualmente pendiente en los tribunales nacionales.

9 » Si tenemos un ordenador de sobremesa encendido durante las 24 horas del día y dedicado exclusivamente a minar bitcoins, su consumo aproximado será de 220 Wh (dentro de una horquilla muy amplia de entre 50 y 450 Wh según el tipo de procesador, los ventiladores, etc.). Si lo extendemos durante toda una semana y lo transformamos a kWh (la unidad de medida de tu consumo eléctrico) nos salen aproximadamente 40 kWh de gasto semanales, si estuvieses en el mercado regulado y tomando como referencia el precio medio de la electricidad en el momento de escribir este post (0,11485 kWh) te salen 4,25 euros de gasto semanal minando bitcoins. Para que el balance sea positivo, la ganancia ha de ser superior. Fuente: https://www.endesa.com/es/blog/blog-de-endesa/luz/cuanta-electricidad-gasta-minar-bitcoins

10 » "Token" se define como "unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas" (Mougayar, 2016)

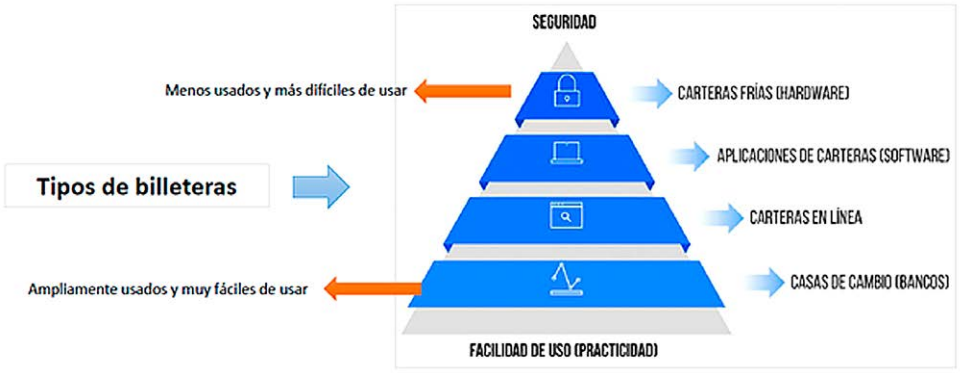


**Figura 3 »** Tipos y características de las wallets (Fuente: https://invertirparaconseguir.com/guia-wallets-criptomonedas/)

Haciendo énfasis en la misma idea, cabe mencionar que las criptomonedas no existen físicamente en los monederos criptográficos, sino que almacenan claves privadas, que recopilan códigos digitales seguros que solo conoce el usuario, y la propiedad de claves públicas, que muestra la misma.[11]

## WALLETS, ICO´S Y TOKENS

### » Wallets de exchanges

Los exchanges, funcionan como bancos de criptomonedas para intercambiar monedas digitales por monedas fiduciarias. La principal característica de estos es que son los únicos tipos de wallets de los que no tenemos claves privadas ya que pertenecen al propio *exchange*. En este tipo de wallet, las transacciones no se registran en la cuenta personal del usuario, sino en la blockchain del propio exchange. Los más famosos son *Coinbase*, *Binance*, *Bit2me* o *Kucoin*, etc.

### » Wallets en línea

Ciertas webs permiten a los usuarios controlar su moneda digital separadamente de sus claves privadas sin tener que instalar ningún software. Estas billeteras crean copias de seguridad, es decir, generan claves privadas de 12 a 24 caracteres, que el usuario debe anotar y guardar en cualquier medio, ya sea físico o digital. Las billeteras en línea más utilizadas son Blockchain.info y MyEtherWallet.

### » Wallets app o softwares

Son conocidas como billeteras calientes. Las wallets app o software, es una billetera instalada en una computadora o dispositivo móvil. Su uso está enfocado a visualizar saldos y realizar transacciones. Las carteras más famosas de este tipo son *Exodus*, *MetaMask*, *Electrum* o *Polkadot js*, etc.

### » Wallets Hardware

Este tipo de billetera se denomina *billetera fría*. Son dispositivos físicos similares a pen drives y recopilan claves privadas para cuentas asociadas fuera de la red de internet. Esto permite que las transacciones se firmen sin exponer la clave privada.

La forma en que se usa incluye la conexión a través de USB, que es la forma más segura de proteger las criptomonedas. Las carteras de hardware más utilizadas son Trezor y Ledger.

Las *dapps* son aplicaciones distribuidas que intentan evitar intermediarios aplicando la tecnología *blockchain*, es decir, funcionan con sistemas descentralizados, evitando así la necesidad de terceros. En particular, *Ethereum*, su confianza se basa en la aplicabilidad de los contratos inteligentes, ya que reproducen la lógica de los acuerdos comerciales.

*Ethereum* se posiciona como una plataforma de referencia para las ofertas iniciales de monedas, capaz de levantar importantes cantidades de capital dependiendo de los diferentes proyectos que alberga.

Mientras las aplicaciones distribuidas se ejecuten en la red, la demanda de la moneda será mayor en la propia plataforma. En este caso, la red *Ethereum* tiene *ether* como moneda. Atendiendo a un ejemplo práctico, digamos que Ethereum es un mapa de una ciudad, un DAPP es un vehículo, y el éter representa combustible, por lo que pagamos en éter para usar la red y ejecutar el contrato inteligente, es para encontrar el DAPP. La aplicación práctica de este sistema en el ámbito de las *DeFi* o finanzas descentralizadas (Tapscott & Tapscott, 2017).

Una ICO es el proceso de distribuir tokens y buscar financiación para ellos en las primeras etapas del desarrollo de un proyecto. Aquellos que obtengan el token podrán usarlo más adelante en el proyecto. Las ICO permiten financiar una idea por un corto período de tiempo. Su prosperidad los ha asimilado a las startups. El proyecto ICO más famoso es *Ethereum*, que es responsable no solo de los nuevos usos de la tecnología *blockchain*, sino también de la forma de su financiación. La ICO logró recaudar $19 millones en

**11 »** Se pueden transferir criptodivisas como cualquier otro activo, al igual que con una transferencia bancaria. La aplicabilidad es básicamente la misma.

fondos un año antes de su lanzamiento, gracias a la extracción previa de sus tokens y su venta.

Los tokens no fungibles, conocidos por el acrónimo NFT, significan tokens digitales únicos y no repetibles. Utilizan tecnología blockchain para garantizar que pertenecen a un único usuario y su autenticidad. La característica principal de estos tokens es que cualquiera puede crearlos usando imágenes, video, audio, URL e incluso objetos físicos en el mundo real. Se diferencian de los tokens fungibles (Bitcoin o cualquier otra criptomoneda) porque se pueden dividir en un mismo token o reemplazar por otro token con las mismas características.

Por otro lado, los NFT´s son únicos e indivisibles. La propia tecnología *blockchain*, a través de contratos inteligentes, proporciona los metadatos necesarios para garantizar su autenticidad. Estos metadatos incluyen: *autor*, *características*, *características* o *rareza de la imagen*.

La dirección del contrato que permite identificar la autenticidad de cada pieza, los royalties que puede recibir el creador cada vez que vende su *NFT*, la posibilidad de determinar el precio inicial, precio de compra, número de transacciones de mercado, etc. (figura 4). En definitiva, un token no fungible se representa a sí mismo como un certificado digital de autenticidad y propiedad para el usuario.

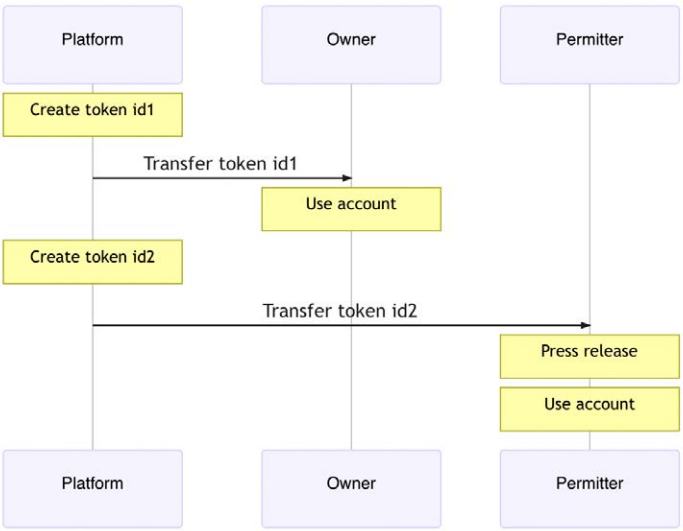


**Figura 4 »** Esquema de creación y transferencia de NFT[13]
(Fuente: https://genobank.io/biosample-permission-token-with-non-fungible-tokens)

## PRINCIPALES CRIPTOMONEDAS

Como recordatorio, debemos señalar las diferencias que encontramos entre las monedas fiduciarias y las criptomonedas. Principalmente, las criptomonedas son monedas digitales descentralizadas, por lo que no están protegidas por los bancos; en cambio, se sabe que las monedas tradicionales son emitidas por agencias gubernamentales y controladas por los bancos. Otra diferencia es la volatilidad de las criptomonedas, cuyo valor fluctúa en exceso debido a la oferta y la demanda. Sin embargo, la moneda FIAT es más estable porque está regulada y establecida por el mercado.

Aunque no lo parezca, tienen similitudes y pueden llamarse monedas, siempre que ambas partes las acepten, pueden ser utilizadas como medio de pago para la compra de bienes o servicios entre usuarios. Antes de invertir en una criptomoneda en particular, debemos comprender su libro blanco o *whitepaper*[12] para asegurarnos de saber cómo funciona y con qué propósito se creó. En términos de definir sus objetivos y características, sepa que todas las criptomonedas no son iguales entre sí. El whitepaper detallará el proyecto, sus objetivos y para qué fue creado, por lo que conoceremos al equipo de trabajo que lo creó, los usuarios previstos o el propósito.

### Bitcoin

La moneda de la que nacen todas es Bitcoin, cuyas siglas son BTC, que, como ya hemos señalado, fue creada por Satoshi Nakamoto, cuya identidad desconocemos y asimilada en un amplio grupo de trabajo. Así lo describió en 2008 la idea de Bitcoin a través de la tecnología *blockchain* como capaz de evitar el doble gasto en redes P2P, es decir, el doble gasto entre partes.

También hay que tener en cuenta que todas las criptomonedas tienen un marco común, no requieren una entidad bancaria central ya que están descentralizadas y sus usuarios pueden ser anónimos. Por ello, *Bitcoin* es la primera moneda digital donde podemos enviar y recibir dinero sin intermediarios.

Para evitar el fraude, existen las l*lamadas pruebas de trabajo* como un arma visionaria, para evitar el doble gasto y para buscar nuevas monedas en el mercado.

12 » Disponible en https://bitcoinwhitepaper.co/

13 » Para implementar la plataforma de permisos básica anterior usando un sistema de cadena de bloques, es necesario implementar tres características:

1. La plataforma asignará identidades de forma seudónima a los propietarios y pública mente a los autorizados mediante criptografía de clave pública.
2. La plataforma asignará identificadores de propiedad a los propietarios después de verificar la propiedad/autorización.
3. Cualquiera puede convertirse en un autorizador mediante la creación de cualquier permiso de cualquier propiedad a cualquier permisionario.

Debido a que este es un sistema de cadena de bloques, se supone que todas las operaciones de solo lectura son gratuitas:

a. Cualquiera puede encontrar la identidad seudónima del dueño de la propiedad.
b. Cualquiera puede verificar el estado actual de cualquier permiso, recursivamente, de vuelta al dueño de la propiedad.

Después de BTC, se han creado miles de criptomonedas diferentes y actualmente hay más de 10.000 criptomonedas en el mercado. Sin embargo, 13 años después, Bitcoin sigue siendo la criptomoneda líder, y lo es en parte por una serie de características que debemos conocer sobre Bitcoin:

» limitación: Bitcoin no podrá superar los 21 millones de BTC e n el mercado.

» fraccionamiento: un BTC se puede dividir en hasta 100 000 000 unidades más pequeñas. La unidad fraccionaria se llama "satoshis" y es igual a 0.00000001 BTC.

» control descentralizado.

La siguiente imagen muestra un ejemplo de una transacción BTC, el número 1 refleja el identificador único de la transacción, el número 2, la dirección original, el número 3, el destinatario, el monto transferido y la misma fecha.


**Figura 5 »** Ejemplo de transacción lineal bitcoin
(Fuente: Bit2me.com)

### Altcoin

Es la principal de la primera serie de monedas alternativas o *altcoins*. Estas se caracterizan por ser toda moneda distinta a bitcoins. *Bitcoin* fue la primera, pero desde su fundación se crearon muchas otras criptomonedas.

### Ether

*Ether* es la moneda de *Ethereum* y es la segunda criptomoneda en sobresalir y mostrarse en el tráfico. Hay una diferencia entre *bitcoin* y *ether*, de hecho, el tiempo que tarda un minero en confirmar y verificar un bloque en el caso de bitcoin es de aproximadamente 10 minutos, mientras que *ether* es de solo 16 segundos. La recompensa para los mineros que obtienen estas pruebas de trabajo es que su éter permanece sin cambios, mientras que su valor en bitcoins disminuye. Asimismo, se sabe que *bitcoin* tiene un límite máximo de 21 millones de monedas, mientras que en el caso del *ether* no existe dicho límite. Este detalle es crucial porque con Bitcoin, cada unidad debe tener un valor más alto, mientras que Ether es un número inflacionario más alto de unidades monetarias, lo que reduce el valor de cada una.

Los inversionistas afectados por estos sistemas inflacionarios o deflacionarios deben tomar en cuenta la moneda ya que de ella depende el uso, ya sea comprando o invirtiendo. Cada criptomoneda viene con un contrato inteligente o Smart contract como hemos visto a lo largo del artículo. Estos contratos inteligentes están vinculados a una marca llamada token. Este token identifica de forma única cada contrato adquirido. Son programas inteligentes capaces de ejecutar transacciones en el supuesto de que cumplan un conjunto de requisitos que decide el creador del contrato.

Otro nombre oficial en el campo de las criptomonedas es Vitalik Butlin, creador y fundador de *Vengeance*, cuyas aportaciones han marcado una gran diferencia en el mundo de las criptomonedas. La mayoría de las altcoins existentes han utilizado el protocolo Ethereum como su fórmula de moneda. *Ripple* (XRP) o *Litecoin* se destacan por la velocidad de las transacciones.

### Litecoin

Por su parte, *Litecoin* es una moneda basada en la programación de *Bitcoin*, pero incluye una versión más ligera, rápida y con una serie de modificaciones de parámetros, capaz de validar transacciones en 2 minutos en lugar de 10. En comparación, su producción alcanzará los 84 millones de monedas 21 bitcoins, es decir, la cifra que alcanzará al multiplicar 4 bitcoins como moneda en circulación.

De la misma forma se han creado miles de criptomonedas, pertenecientes a una blockchain específica que ya existe y cuya tecnología ha sido modificada para desarrollar funcionalidades que la hagan más activa.

## OTRAS CRIPTOMONEDAS RELEVANTES

Como se mencionó a lo largo del artículo, hay muchas criptomonedas, hasta más de 10,000, por lo que se invita a profundizar en la alteridad disponible,[14] si bien las principales son en la actualidad:

**Cardano**, una moneda que ha crecido mucho en los últimos meses, es conocida como la moneda representativa de la cadena de bloques de tercera generación.

**Tether** o **USD Coin**, son monedas conocidas como stable coins o monedas estables, lo que significa que su valor no cambia y es igual a 1 USD

**Binance Coin** nació para respaldar las operaciones en la plataforma de criptomonedas que lleva el nombre de Binance.

**Ripple (XRP)** se conoce como una alternativa a Bitcoin. Esto permite transacciones globales más flexibles y rentables.

**14 »** Existen multitud de portales para transacción CEX o DEX, como https://coinmarketcap.com/all/views/all/

## CONCLUSIONES

A diferencia de lo que sucede con la moneda fiduciaria, que se puede generar en cualquier momento -sin embargo, esto hace que pierda su valor porque hay más moneda en circulación- esto no sucede con las criptomonedas, puesto que se han fijado límites para acuñar monedas, y esto se espacia en el tiempo.

A diferencia de lo que sucede con la moneda fiduciaria, que se puede generar en cualquier momento mediante los correspondientes acuerdos de países y organismos según sus posibilidades y necesidades, por el contrario esto no sucede con las criptomonedas, puesto que se han fijado límites para acuñar monedas, y esto se espacia en el tiempo.

Las criptomonedas, a su vez, no tienen deuda, a diferencia de lo que la ciudadanía asume contrae cuando tomamos un préstamo para comprar un automóvil o una casa. La producción de criptomonedas es limitada y su cantidad es solo cierta y constante.

Por otro lado, hay disponible una cantidad variable de monedas. La frecuencia y forma de estas emisiones no están centralizadas y no dependen de la organización que las emite, sino que la propia comunidad conduce a la creación de nuevas monedas a través de la minería a través de transacciones verificadas, controlando siempre a los mismos usuarios.

Además de esto, existen otro tipo de criptomonedas creadas por las empresas responsables de sus proyectos. Estos los explotan y si no son útiles para el usuario, eventualmente desaparecerán o tendrán un valor cero.

Gracias a la tecnología blockchain, la transacción a ejecutar debe ser verificada por toda la comunidad y los usuarios que la componen (Sánchez Smith, 2021). Si algún día todos los usuarios deciden retirar su criptomoneda de la red, podrán hacerlo sin perder ninguna cantidad. Algo que no se puede confirmar en el mundo centralizado en el que vivimos.

## REFERENCIAS BIBLIOGRÁFICAS


ETSI (2019) ***White Paper N.32 Ne***V

Almonacid Sierra, J. J. (2020). ***Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado***. Revista de Derecho Privado(38), 119-142.

del Pozo, Susana. 2021. ***Blockchain*** en: UEM STEAM essentials (enlace web UEM. Recuperado de https://universidadeuropea.com/conocenos/escuela-arquitectura-ingenieria-diseno-madrid/)

Figuero Castilla, Z. (2020). ***Criptomonedas***. (M. D. Soto, Ed.) Valladolid: Universidad de Valladolid. Obtenido de https://uvadoc.uva.es/handle/10324/46332

Gamage, H. T. (2020). ***A survey on blockchain technology concepts, applications, and issues***. SN Computer Science, 1(2), 1-15.

Lemieux, P. (2013). Who is satoshi nakamoto? Regulation, 36(3), 14-16.

Mougayar, W. (2016). ***The business blockchain: promise, practice, and application of the next Internet technology***. Nueva York: John Wiley & Sons.

Pacheco, G. M. (2020). ***La revolución fintech en los medios de pago: situación actual y perspectivas***. Revista de Estudios Empresariales. Segunda época (2), 112-133.

Sánchez Smith, G. (2021). ***Bitcoin lo cambia todo***. Madrid: Pirámide.

Santos, Leopoldo. 2021. ***Ciberseguridad e infraestructuras críticas*** en: UEM STEAM Essentials (enlace web UEM. Recuperado de https://universidadeuropea.com/conocenos/escuela-arquitectura-ingenieria-diseno-madrid/)

Seok, B., Park, J., & Hyuk, J. (2019). ***A Lightweight Hash-Based Blockchain Architecture for Industrial IoT***. applied sciences, 9(18). doi: https://doi.org/10.3390/app9183740

Silva, P. &. (2018). ***Análisis de la evolución de la criptomoneda bitcoin en el mundo entre el 2010 y el 2018***. Bogotá: Fundación Universidad de América. Obtenido de https://hdl.handle.net/20.500.11839/6923

Swartz, L. (2018). ***What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology***. Cultural Studies, 32(4), 623-650.

Tapscott, D., & Tapscott, A. (2017). ***La revolución Blockchain***. Bilbao: Deusto.


## BIOGRAFÍA

Nacido en Santa Cruz de Tenerife en 1987. Diplomado en Ciencias Empresariales por la Universidad La Laguna posee dos títulos de Máster: en Asesoría Fiscal y Contable (ULL) y en Protección de Datos (UNIR), Doctorando en Derecho y nuevas tecnologías (UNIR). Asesor fiscal y en materia de protección de datos. Socio director de la firma CRUZ ASESORES. Decano del Colegio Oficial de Titulados Mercantiles y Empresariales de Santa Cruz de Tenerife, COTIME. Profesor de la Universidad Europea de Canarias y de la Universidad de La Laguna. Conferenciante y redactor habitual en diferentes foros y medios.