



Centro de Estudios Sociales y de Opinión Pública

Pulso  ciudadano

# Criptomonedas


---

Abril de 2018

La información contenida en este documento es un compendio analítico de estudios de diversas instituciones o empresas, el cual no refleja la opinión del CESOP ni de la Cámara de Diputados.

[www.diputados.gob.mx/cesop](http://www.diputados.gob.mx/cesop)

 @cesopmx

 cesop01



# ÍNDICE

# Índice

---

Tema	Página
Introducción	4
1. Definiciones básicas	5
2. Tipos de criptomonedas	11
3. Capitalización de mercado de las criptomonedas	24
4. Plataformas de Bitcoin en el mercado	28
5. Regulación de criptomonedas en México	31

## Introducción

Las criptomonedas son una innovación tecnológica que operan como cualquier moneda, la más conocida es el Bitcoin; sin embargo, existen muchas más.

En la actualidad ya hay diferentes lugares en donde puedes pagar con bitcoins, un ejemplo de esto es la iniciativa “Calle Bitcoin” en Madrid y Barcelona, la cual promueve que puedas pagar en establecimientos con este tipo de moneda; en Madrid más de 20 establecimientos en la calle Serrano acepta este tipo de pagos, y en Barcelona se encuentra en la zona de Ciutat Vella.

Cada vez hay más proveedores que aceptan bitcoin como forma de pago. Ya pueden comprarse todo tipo de productos y servicios con esta moneda: por ejemplo: Microsoft permite comprar apps, juegos o videos en Windows, Windows Phone y Xbox; en Overstock se pueden adquirir joyas, muebles o electrodomésticos; en Showroomprive, empresa de retail europea, puede comprarse cosmética, accesorios o ropa.

Este documento presenta información relacionada con las criptomonedas: su definición y los términos utilizados en este tipo de unidades. De igual manera, se dan a conocer los beneficios y los riesgos de utilizarlas, y las diferencias entre las divisas comunes y este tipo de divisa.

El segundo apartado muestra los 10 tipos de criptomonedas que se encuentran dentro del ranking de las 100 mejores, así como la criptomoneda creada por el gobierno venezolano llamada “El Petro”.

La tercera parte del documento da a conocer el nivel de capitalización de mercado de las 10 mejores criptomonedas; por su parte, en el cuarto apartado se presentan las tres plataformas creadas para gestionar las transacciones del Bitcoin. Finalmente, en la quinta sección se habla de las regulaciones que se establecieron en México para estar a la vanguardia a nivel internacional en materia de regulación de servicios financieros.



# 1. Definiciones básicas

## Criptomonedas

Las criptomonedas son unidades virtuales que pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras.

Son una alternativa de las divisas tradicionales, pero en realidad fueron concebidas como una solución de pago completamente convencional. Aunque su validez como método de pago es fundamental por su valor, habitualmente se parecen más a materias primas. Es decir:

- El valor de una criptomoneda no está vinculado exclusivamente al comportamiento de una economía concreta.
- Los cambios en los tipos de interés y el aumento en las reservas monetarias sólo tienen un efecto indirecto en su valor.
- El valor de las criptomonedas depende del compromiso de los usuarios por mantener su precio al convertirlas a divisas tradicionales.

Esto significa que, por ahora, las criptodivisas son tratadas principalmente como una materia prima, una inversión cuyo retorno proviene de la especulación en torno a las subes y bajas de su valor.

Existe un gran número de criptodivisas disponibles, todas con sus propias características y aplicaciones. Las que tienen mayor capitalización de mercado son: bitcoin, bitcoin cash, ether, litecoin, ripple y dash.

Fuente: Tomado de IG Markets Ltd, *¿Qué son las criptomonedas?*, y de BBVA, *Diccionario básico de "blockchain": diez términos que debes conocer*, 10 de noviembre de 2017, disponible en [www.ig.com](http://www.ig.com) y [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).

## Minería digital

El proceso a través del cual las transacciones de criptomoneda se verifican y ofrecen nuevas unidades se conoce como minar criptomonedas. El objetivo de los mineros es recopilar las últimas transacciones en bloques y encontrar una solución a un complejo algoritmo; para validar cada transacción y crear los bloques los mineros deben encontrar el “hash”, o clave digital, de cada bloque para enlazarlo con el siguiente. Cada vez que los mineros encuentran una de estas claves criptográficas se mina un bitcoin y ellos reciben una retribución en esta misma moneda.

## Blockchain

El *blockchain* o cadena de bloques es un libro digital compartido que registra todas las transacciones de una criptomoneda determinada entre dos pares. Estas transacciones forman agrupaciones conocidas como “bloques”, que a su vez codifican y se vinculan unos a otros.

La información registrada en la cadena de bloques se almacena en millones de ordenadores y está abierta para todo el mundo, en lugar de almacenarse en un solo lugar. Esto hace que el proceso sea transparente e inmune a modificaciones, sin puntos débiles vulnerables al error humano o informático. El blockchain es principalmente una plataforma digital en la que se pueden crear todo tipo de programas: incluye gestión de la identidad, software de seguridad y procesamiento de transacciones.

## Initial Coin Offering (ICO)

Un ICO es la forma en la que los fundadores de una nueva criptomoneda obtienen capital para su proyecto, a cambio de tokens de su divisa. El proyecto puede estar destinado exclusivamente a su nueva criptomoneda o puede abarcar otras aplicaciones de blockchain.

Fuente: Tomado de IG Markets Ltd, *¿Qué son las criptomonedas?*, y de BBVA, *Diccionario básico de “blockchain”: diez términos que debes conocer*, 10 de noviembre de 2017, disponible en [www.ig.com](http://www.ig.com) y [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).

Los ICO se están convirtiendo rápidamente en la forma preferida de lanzar una nueva criptomoneda al mercado. La esperanza está en que si la nueva criptomoneda se convierte en el nuevo éxito, ya estará disponible; sin embargo, son una apuesta arriesgada, ya que al contrario de lo que ocurre con compañías que cotizan en bolsa, las nuevas criptomonedas no están probadas en el mercado y no confieren derechos de propiedad. Esto hace que la inversión sea puramente especulativa.

## Tokens

Tradicionalmente, “token” es el nombre con el que se llama a las piezas que, adquiridas a cambio de dinero, sirven para recibir un bien o servicio. Ya sea, por ejemplo, las fichas para jugar en un casino, o para comprar comida en un festival. En el mundo de la cadena de bloques, esta palabra sirve para designar unidades de valor que pueden adquirirse a través de “blockchain” y que se usan para obtener bienes y servicios.

Estas unidades se transmiten a través de los mensajes de la red de “blockchain”, pero a diferencia de la moneda, sirven para intercambiarse por todo tipo de servicios. Dentro de una red privada un “token” puede servir para otorgar un derecho, pagar por un trabajo o ceder unos datos como incentivo; es la puerta de entrada a servicios extra o a una mejor experiencia de usuario. Incluso pueden usarse como garantía de la recepción de futuros servicios que una compañía promete ofrecer, cuando se usan en las ICO como forma de financiación de “startups”.

Fuente: Tomado de IG Markets Ltd, *¿Qué son las criptomonedas?*, y de BBVA, *Diccionario básico de “blockchain”: diez términos que debes conocer*, 10 de noviembre de 2017, disponible en [www.ig.com](http://www.ig.com) y [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).



## 1.1 Beneficios y riesgos

Algunos de los beneficios que se obtienen de las criptomonedas son:

- **Visión global:** las criptomonedas son divisas globales, mucho menos susceptibles a la economía o políticas de un país concreto. Todo el mundo puede acceder a ellas y pueden transferirse instantáneamente a cualquier persona en cualquier lugar del mundo.
- **Volatilidad:** suelen experimentar significativos movimientos de precio de manera repentina. Esto las hace problemáticas como divisa pero muy interesantes por las oportunidades de *trading* que ofrecen.
- **Descentralización:** las criptomonedas están descentralizadas; no existe un mercado oficial, lo que significa que pueden ser operadas 24 horas al día durante los siete días de la semana.
- **Transparencia:** todas las transacciones se registran en un libro compartido y se operan sobre un mecanismo que asegura que al receptor sólo le llegue la información que necesita del emisor, no todos sus datos.

Mientras que algunos de los riesgos son:

- **Volatilidad:** la volatilidad puede conllevar tanto riesgos como oportunidades, las grandes fluctuaciones de los precios pueden traer pérdidas de cientos de dólares durante la noche.
- **Amplia aceptación:** las criptomonedas tienen el valor que se les quiera dar, a pesar de su creciente popularidad, aún hay dudas sobre su futuro a largo plazo.
- **Pérdidas:** no hay una manera perfecta de protegerse frente al error humano, el fallo técnico o el fraude, y no hay ningún sistema implantado para compensarle por sus pérdidas.
- **Cambios regulatorios:** las criptomonedas están exentas de regulación por ahora, pero si se introducen nuevos mecanismos, muchas de sus ventajas sobre las divisas tradicionales pueden verse revertidas.

Fuente: Tomado de IG Markets Ltd, *¿Qué son las criptomonedas?*, y de BBVA, *Diccionario básico de "blockchain": diez términos que debes conocer*, 10 de noviembre de 2017, disponible en [www.ig.com](http://www.ig.com) y [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).



## Diferencias entre divisas tradicionales y criptomonedas

Algunas de las diferencias más notorias entre las divisas tradicionales y las criptomonedas son: las criptomonedas son digitales y globales, a diferencia de las divisas tradicionales que se encuentran vinculadas a algún país o a un grupo de países y éstas son físicas.

Las criptomonedas se ofrecen a través de la minería, mientras que las divisas tradicionales son emitidas por el gobierno y son controladas por los bancos centrales.

<b>Divisas tradicionales</b>	<b>Criptomonedas</b>
Físicas	Digitales
Vinculadas a un país concreto o grupo de países	Globales
Emitidas por gobiernos	Ofrecidas a través de minería
La oferta la controlan los bancos centrales	La oferta la controlan los mineros y la tecnología de minería
Se inyectan en el sistema económico a través de bonos y otros títulos	Se inyectan directamente en el mercado de criptomonedas
Reciben gran influencia de las tasas de inflación y de interés	Reciben poca influencia de políticas monetarias

Fuente: Tomado de IG Markets Ltd, *¿Qué son las criptomonedas?*, y de BBVA, *Diccionario básico de "blockchain": diez términos que debes conocer*, 10 de noviembre de 2017, disponible en [www.ig.com](http://www.ig.com) y [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).



## 2. Tipos de criptomonedas

Actualmente existen cerca de 1,400 criptomonedas. En este apartado se presentarán únicamente las que se encuentran catalogadas como las 10 mejores por CoinMarketCap. Asimismo, se dará a conocer la criptomoneda creada por el gobierno venezolano.

## 2.1 Bitcoin

Es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Fue creado por Satoshi Nakamoto en 2009; sin embargo, Satoshi abandonó el proyecto a finales de 2010, y desde entonces la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin.

Bitcoin es una aplicación móvil o de escritorio que provee un monedero personal y permite al usuario enviar y recibir bitcoins con él. La red Bitcoin comparte una contabilidad pública llamada “blockchain”; ésta contiene cada transacción procesada, permitiendo verificar la validez de cada transacción; la autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío, permitiendo a todos los usuarios tener control total al enviar bitcoins desde sus direcciones Bitcoin.

A finales de agosto de 2013, el valor de todos los bitcoins en circulación superaba los 1.5 billones de dólares y cada día se intercambiaban el equivalente a millones de dólares en bitcoins. Los bitcoins se adquieren de cuatro formas distintas:

Fuente: Tomado de Bitcoin, *Mitos y preguntas comunes sobre Bitcoin*, disponible en [www.bitcoin.org](http://www.bitcoin.org) (fecha de consulta: marzo de 2018).

- Como pago de bienes o servicios.
- Comprar en una casa de cambio de Bitcoin.
- Intercambio de bitcoins con alguna persona de su zona.
- Consiguiendo bitcoins a través de la competitiva minera.

El precio del bitcoin se determina por la oferta y la demanda; cuanto la demanda se incrementa el precio sube, y cuando cae la demanda, el precio cae. Hay un número limitado de bitcoins en circulación y los nuevos bitcoins se crean a una velocidad predecible y decreciente, esto significa que la demanda debe seguir este nivel de inflación para mantener un precio estable.

### **Legalidad**

Hasta la fecha, el bitcoin no se ha hecho ilegal por la ley que existe en la mayoría de los territorios; sin embargo, en Tailandia se puede limitar la concesión de licencias a ciertas entidades como son las casas de cambio de bitcoins. Reguladores de varias zonas están tomando medidas para proveer a individuos y negocios con reglas acerca de cómo integrar esta nueva tecnología; la Red de Protección de Crímenes Financieros (FinCEN), oficina del Ministerio de Hacienda de Estados Unidos, emitió una guía sobre cómo caracterizan ciertas actividades que involucran monedas virtuales.

El Bitcoin está diseñado para dar un paso adelante en la seguridad monetaria, ya que son imposibles de falsificar. Los usuarios tienen control total sobre sus pagos y no pueden recibir cobros no aprobados como los que pueden verse con tarjetas de crédito. Las transacciones Bitcoin son irreversibles e inmunes a devoluciones fraudulentas, ya que permite asegurar el dinero contra robo utilizando fuertes y útiles mecanismos como las copias de seguridad, el cifrado criptográfico y las firmas múltiples.

Fuente: Tomado de Bitcoin, *Mitos y preguntas comunes sobre Bitcoin*, disponible en [www.bitcoin.org](http://www.bitcoin.org) (fecha de consulta: marzo de 2018).

## 2.2 Ethereum

Ethereum es una plataforma descentralizada que realiza contratos inteligentes: aplicaciones que ejecutan exactamente como se programaron sin posibilidad de tiempo de inactividad, fraude, censura, o interferencia de terceros. Estas aplicaciones se ejecutan en una cadena de bloques personalizada, una infraestructura global compartida enormemente poderosa que puede mover el valor y representar la propiedad de la propiedad.

La Ethereum Wallet es una puerta de entrada a aplicaciones descentralizadas en la cadena de bloques de Ethereum. Le permite mantener y proteger el ether y otros criptoactivos creados en Ethereum, así como escribir, implementar y usar contratos inteligentes.

El Ether es un elemento necesario para operar la plataforma distribuida de la aplicación Ethereum. Es una forma de pago creada por los clientes de la plataforma a las máquinas que ejecutan las operaciones solicitadas. En otras palabras, ether es el incentivo que asegura que los desarrolladores escriban aplicaciones de calidad y que la red se mantenga saludable.

El suministro total de ether y su tasa de emisión se decidieron por donaciones reunidas en la preventa de 2014. Los resultados fueron aproximadamente:

- 60 millones de ether creados para los contribuyentes de la preventa.
- 12 millones (20% de lo anterior) fueron creados para el fondo de desarrollo: la mayor parte se destinará a los primeros contribuyentes y desarrolladores, y el resto a la Fundación Ethereum.
- Se crean 5 ethers por cada bloque (aproximadamente 15 segundos) para el minero del bloque.

Fuente: Tomado de Ethereum, *Preguntas frecuentes*, disponible en [www.ethereum.org](http://www.ethereum.org) (fecha de consulta: marzo de 2018).

- De dos a tres ethers en ocasiones se envían a otro minero. Ellos fueron capaces de encontrar una solución, aunque su bloque no se incluyó.

La red Ethereum funciona con computadoras de todo el mundo. Para recompensar los costos computacionales de procesar los contratos y asegurar la red, existe una recompensa que se otorga a la computadora que fue capaz de crear el último bloque de la cadena. Cada 15 segundos, en promedio, un nuevo bloque se agrega a la cadena con las últimas transacciones procesadas por la red y la computadora; lo que genera este bloque se premia con tres ethers. Debido a la naturaleza del algoritmo para la generación de bloques, este proceso (que genera una prueba de trabajo) garantiza que es aleatorio y los premios se dan en proporción al poder computacional de cada máquina.

## 2.3 Ripple

Ripple es el activo digital más rápido y escalable, lo que permite pagos globales en tiempo real en cualquier parte del mundo. Fue construido para uso empresarial; ofrece a los bancos y proveedores de pagos una opción confiable a pedido con la finalidad de obtener liquidez para pagos transfronterizos. Utiliza tecnología de código abierto, basada en los principios de blockchain con un conjunto creciente de validadores.

Los proveedores de pago utilizan ripple para ampliar su alcance a nuevos mercados, reducir los costos de divisas y proporcionar una liquidación de pagos más rápida.

Ripple maneja consistentemente 1,500 transacciones por segundo, 24x7 y puede escalar para manejar el mismo rendimiento que Visa. Los pagos se liquidan en 4 segundos. Ripple está disponible para su compra en más de 60 intercambios de activos digitales en todo el mundo.

Fuente: Tomado de Ethereum, *Preguntas frecuentes*, y de Ripple, *Preguntas frecuentes*, disponible en [www.ethereum.org](http://www.ethereum.org) y en <https://ripple.com> (fecha de consulta: marzo de 2018).

## 2.4 Bitcoin Cash

Bitcoin Cash es dinero electrónico de usuario a usuario a través de internet. Es completamente descentralizado; no existe ningún banco central y funciona sin requerir confianza en ningún tercero. Es la continuación del proyecto Bitcoin como dinero digital de usuario a usuario; es una bifurcación de la blockchain de Bitcoin, con reglas de consenso actualizadas que le permiten crecer y escalar.

Todas las personas que poseían Bitcoins al momento de la creación de Bitcoin Cash, pasaron a tener esa misma cantidad en Bitcoin Cash. Esto significa que todo el que poseía Bitcoin del bloque 478558, el 1 de agosto de 2017, obtuvo una cantidad de Bitcoin Cash equivalente a la que tenía de Bitcoin en ese momento. Todas las transacciones de Bitcoin y Bitcoin Cash posteriores al 1 de agosto de 2017 son totalmente independientes.

Características:

- **Escalabilidad on-chain:** Bitcoin cash se mantiene fiel a la hoja de ruta de Nakamoto de conseguir la adopción global al escalar on-chain (en la cadena). Como primer paso se implementó un límite del tamaño del bloque ajustable, con una capacidad estándar aumentada a 8MB.
- **Nuevas firmas digitales:** un nuevo tipo de SigHash proporciona replay protection (protección frente a transacciones repetidas), mayor seguridad en monederos hardware, y la eliminación del problema de hashing cuadrático.
- **Nuevo algoritmo de ajuste de la dificultad:** Un ajuste reactivo de la dificultad de Proof-of-Work permite a los mineros migrar desde la cadena antigua de Bitcoin según lo deseen, a la vez que ofrece protección frente a fluctuaciones en la tasa de hash.
- **Desarrollo descentralizado:** el futuro está a salvo gracias a que son múltiples equipos independientes de desarrolladores los que ofrecen las implementaciones del software. Bitcoin Cash es resistente a ataques políticos y sociales al desarrollar el software.

Fuente: Tomado de Bitcoin Cash, *Acerca de y características*, disponible en [www.bitcoincash.org](http://www.bitcoincash.org) (fecha de consulta: marzo de 2018).



## 2.5 Litecoin

Litecoin es una moneda de internet de tipo punto a punto que permite realizar pagos instantáneos y de costo casi cero a cualquier parte del mundo. Es una red de pagos global y de código abierto que es completamente descentralizada y sin autoridades centrales. Litecoin provee tiempos de confirmación de transacciones más rápidas y eficiencia de almacenamiento mejorada sobre la principal moneda basada en matemáticas. Es un medio de comercio comprobado complementario a Bitcoin.

Litecoin es un proyecto de software libre publicado bajo la licencia MIT/X11 que otorga la posibilidad de ejecutar, modificar, copiar y distribuir el software, a discreción, en copias modificadas del mismo. El software es lanzado en un proceso transparente que permite la verificación independiente de binarios y su correspondiente código fuente.

La cadena de bloques de litecoin es capaz de administrar un mayor volumen de transacciones que Bitcoin; debido a que la generación de bloques se realiza de manera más frecuente, la red sustenta más transacciones sin la necesidad de modificar el software en el futuro.

El cifrado de la cartera electrónica permite asegurar las claves privadas en ella, para que uno pueda ver las transacciones y su saldo de cuenta, pero se solicita el ingreso de contraseña antes de utilizar sus litecoins. Esto es útil no sólo como protección ante los virus y troyanos, sino también como una comprobación de seguridad antes de enviar un pago.

Inicialmente, los mineros pueden generar 25 monedas por bloque; la cantidad de monedas generadas se ve reducida a la mitad cada 4 años (840,000 bloques); por tanto, la red Litecoin está programada para producir aproximadamente 4 veces más unidades monetarias que Bitcoin, o cerca de 84 millones de litecoins.

## 2.6 Cardano

Cardano es un proyecto de cadena de bloques y criptomonedas público, descentralizado y de código abierto. Cardano está desarrollando una plataforma de contrato inteligente que busca entregar características más avanzadas que cualquier protocolo desarrollado previamente. Es la primera plataforma de blockchain que evoluciona a partir de una filosofía científica y un enfoque impulsado por la investigación. El equipo de desarrollo consiste en un gran colectivo global de ingenieros expertos e investigadores.

## 2.7 NEO

NEO es un proyecto de cadena de bloques basado en la comunidad, sin fines de lucro. Es una red distribuida que realiza “economía inteligente”, al digitalizar activos con tecnología blockchain e identidades digitales, y automatizar la gestión de activos digitales mediante contratos inteligentes.

NEO comenzó formalmente su proyecto en 2014 y abrió sus puertas en tiempo real en Github en junio de 2015. Desde su creación, el equipo de NEO ha sido testigo de los altibajos de la industria de las cadenas de bloques, del frenesí y enfriamiento del mercado monetario digital. En NEO creen que la ciencia y la tecnología son la motivación detrás de los cambios en esta era.

NEO admite una variedad de activos digitales. Los usuarios pueden registrar sus propios NEO en la distribución de activos, libre comercio y circulación.

Fuente: Tomado de Cardano Hub, *Cardano*, y de NEO, *Qué es NEO*, disponible en [www.cardanohub.org](http://www.cardanohub.org) y en <https://neo.org> (fecha de consulta: marzo de 2018).

## 2.8 Stellar

Stellar es una plataforma que conecta bancos, sistemas de pagos y personas. Se integra para mover dinero de manera rápida, confiable y casi sin costo. Las diferencias entre la red de Stellar y Bitcoin son las siguientes:

- Stellar está basado en un consenso algorítmico en lugar de la minería. Esto significa que las transacciones se confirman en pocos segundos.
- El suministro de lumen aumenta a una tasa fija de 1% por año.
- Stellar tiene como objetivo permitirle realizar transacciones en la moneda de su elección.

La esperanza es que la divisa en sí misma sea principalmente una moneda detrás de escena y que la red Stellar ayude a proporcionar más liquidez entre las monedas. Con un equipo de profesionales de alta tecnología y finanzas, la organización sin fines de lucro Stellar.org amplía el acceso a servicios financieros de bajo costo para luchar contra la pobreza y maximizar el potencial individual.

Los lumens son el activo nativo de la red Stellar; esto quiere decir que los lumens se crean dentro de la red.

En 2014 esta red lanzó 100 mil millones de stellars. En 2015, con el lanzamiento de la red mejorada, el nombre del activo cambio de stellar a lumen, con el fin de distinguirlo de la red Stellar y de Stellar.org (la organización sin fines de lucro que contribuye al desarrollo de la red).

La red Stellar ofrece todas las características innovadoras de un libro público compartido en una base de datos distribuida, a menudo denominada tecnología blockchain. El lumen tiene dos propósitos:

Fuente: Tomado de Stellar, *Preguntas frecuentes*, disponible en [www.stellar.org](http://www.stellar.org) (fecha de consulta: marzo de 2018).

1. Los lumens juegan un pequeño rol anti spam: cada transacción tiene una tarifa menor (0.00001 lumens) asociada a ella. Esta tarifa evita que los usuarios con intenciones maliciosas inunden la red (conocido como ataque DoS). Los lumens funcionan como un token de seguridad, mitigando los ataques DoS que intentan generar grandes cantidades de transacciones o consumen grandes cantidades de espacio en el libro mayor.
2. Los lumens pueden facilitar las transacciones en varias monedas: a veces facilitan los intercambios entre pares de unidades, los cuales no tienen un gran mercado directo que actúe como un puente. Esta función es posible cuando hay un mercado líquido entre el lumen y cada moneda involucrada.

## 2.9 MONERO

Monero es una moneda privada, segura y no rastreable. Es de código abierto y está disponible para todos. Es una criptomoneda descentralizada. Es decir, es dinero digital seguro operado por su propia red de usuarios. Las transacciones son confirmadas por consenso distribuido y luego registradas inmutablemente en la cadena de bloques. De esta manera, mantiene tu dinero seguro sin necesidad de terceras partes.

Usa las tecnologías de firmas de círculo y transacciones confidenciales de círculo (RingCT) para ofuscar el importe, origen y destino de cada transacción. Monero ofrece los beneficios de una criptomoneda descentralizada sin comprometer la privacidad y es fungible porque es privada por defecto.

Fuente: Tomado de Stellar, *Preguntas frecuentes*, y de Monero, *Monero*, disponible en [www.stellar.org](http://www.stellar.org) y en <https://getmonero.org> (fecha de consulta: marzo de 2018).

## 2.10 Dash

Dash es una criptomoneda de fuente abierta entre pares con un fuerte enfoque en la industria de pagos. Dash ofrece una forma de dinero que es portátil, económica, divisible y rápida. Se puede gastar de forma segura tanto en línea como en persona sólo con tarifas de transacción mínimas. Basado en el proyecto Bitcoin, Dash pretende ser el sistema de pagos más escalable y fácil de usar en el mundo. Además del conjunto de características de Bitcoin, Dash actualmente también ofrece transacciones instantáneas (InstantSend), transacciones privadas (PrivateSend). Opera un modelo autónomo y autofinanciado que permite a la red Dash pagar a individuos y a empresas por un trabajo que agrega valor a la red. Este sistema de gobernanza y presupuesto descentralizado lo convierte en una de las primeras organizaciones autónomas descentralizadas exitosas (DAO).

## 2.11 Petro

El Petro es el primer criptoactivo emitido por un estado. Esta criptomoneda estará respaldada por la República Bolivariana de Venezuela y la riqueza de sus grandes reservas de petróleo crudo. Tiene su origen en la idea del presidente Hugo Chávez.

El Petro fue creado de manera innovadora, utilizando los más altos estándares en tecnología de cadena de bloques y seguridad de la información; pensando en un futuro donde las representaciones electrónicas de activos faciliten un comercio más directo entre naciones emergentes, así como la labor del Estado en el marco de una independencia financiera y económica.

Durante los últimos cuatro años Venezuela ha experimentado la mayor crisis financiera de su historia, resultado de una devaluación de su moneda nacional, el bolívar. Con la finalidad de fortalecer la soberanía monetaria y promover el bienestar, el gobierno venezolano decidió embarcarse en un proyecto de futuro con la visión de convertir al país en un centro de creación de soluciones basadas en la tecnología de cadenas de bloques para las economías emergentes.

Fuente: Tomado de Dash, *Dash*, y de Petro, *El criptoactivo de la República Bolivariana de Venezuela. Propuesta financiera y tecnológica*, disponible en [www.dash.org](http://www.dash.org) y en [www.elpetro.gob.ve](http://www.elpetro.gob.ve) (fecha de consulta: marzo de 2018).

El Petro impulsará el surgimiento de un sistema financiero global más justo, colaborativo, autónomo, favorable al crecimiento y al intercambio entre economías en desarrollo. Tendrá tres facetas:

1. Medio de intercambio: podrá ser usado para adquirir bienes o servicios y será canjeable por dinero fiduciario, y otros criptoactivos o criptomonedas a través de casas de intercambio digitales.
2. Plataforma digital: podría ejercer las funciones de una representación digital de mercancías y/o materias primas y servirá como andamio para crear otros instrumentos digitales orientados al comercio y las finanzas nacionales e internacionales.
3. Instrumento de ahorro e inversión: su valor estable alentará su uso como reserva de valor e inversión financiera.

El total de Petro emitido y puesto a la venta será de cien millones, no habrá emisiones extraordinarias. Éste será divisible en 100,000,000 de unidades. La unidad mínima de intercambio será denominada Mene (0.00000001).


La preventa del Petro inició el 20 de febrero de 2018 y consistió en la creación y venta de un activo inteligente (Smart Asset) sobre la cadena de bloques de la plataforma NEM. Este proceso promoverá y garantizará demandantes para la oferta inicial que se realizará posteriormente. Los token que cumplen con las exigencias del “mosaic” sobre el estándar de la cadena de bloques NEM son fichas digitales no minables que se emiten en su totalidad a través de un contrato inteligente en dicha plataforma. El token podrá ser canjeado por Petro en cualquier momento entre la fecha de lanzamiento y el cierre de la oferta inicial. La oferta inicial se realizará posteriormente hasta agotar los 82 millones 400 mil unidades disponibles para la venta.

Fuente: Tomado de Petro, *El criptoactivo de la República Bolivariana de Venezuela. Propuesta financiera y tecnológica*, disponible en [www.elpetro.gov.ve](http://www.elpetro.gov.ve) (fecha de consulta: marzo de 2018).

## Preventa y oferta inicial del Petro

Preventa	Oferta inicial
Tokens disponibles: 38,400,000	Total de Petro disponible para la venta: 44,000,000
Precio de venta de referencia: USD 60	Precio de venta de referencia: USD 60
Fecha y hora de inicio: 20 de febrero de 2018 a las 8:30 am (hora de Venezuela)	Fecha y hora de inicio: 20 de marzo de 2018 a las 23:59:59 pm (hora de Venezuela)
Fecha y hora de cierre: 19 de marzo de 2018 a las 23:59:59 pm (hora de Venezuela)	Fecha y hora de cierre: hasta agotarse los Petro de la emisión inicial.

Fuente: Tomado de Petro, *El criptoactivo de la República Bolivariana de Venezuela. Propuesta financiera y tecnológica*, disponible en [www.elpetro.gob.ve](http://www.elpetro.gob.ve) (fecha de consulta: marzo de 2018).



# 3. Capitalización de Mercado de Criptomonedas



La capitalización de mercado es una forma de clasificar la dimensión relativa de una criptomoneda; ésta se calcula multiplicando el precio por las acciones en circulación.

Los precios de las diferentes criptomonedas se calculan tomando el precio ponderado de todos los precios declarados de cada mercado.

Para que una criptomoneda esté en la lista de CoinMarketCap, debe cumplir con lo siguiente:

- Ser una criptomoneda o un token de cifrado.
- Estar a la venta al público con un API que informe el último precio cotizado y el volumen de comercio de las últimas 24 horas.
- El volumen de comercio debe tener un saldo diferente a cero en al menos un cambio financiado para que así se pueda determinar el precio.
- Para la clasificación de capitalización de mercado se requiere una figura precisa de acciones en circulación.

Las acciones en circulación son la mejor aproximación del número de monedas que están circulando en el mercado y en las manos del público en general; se utilizan para determinar la capitalización de mercado, ya que es una mejor medida para determinar la capitalización bursátil. Las monedas que están bloqueadas, reservadas o que no se pueden vender en el mercado público, son monedas que no pueden afectar al precio y, por tanto, no se debe permitir que afecten a la capitalización del mercado.

Fuente: Tomado de CoinMarketCap, *Capitalización de Mercado de Criptomoneda, preguntas frecuentes*, disponible en [www.coinmarketcap.com/es](http://www.coinmarketcap.com/es) (fecha de consulta: marzo de 2018).

CoinMarketCap enlista un total de 1,556 criptomonedas en el mercado, de las cuales muestra su precio, capitalización de mercado y las acciones en circulación. De acuerdo con las cifras obtenidas en este sitio web, se tiene al 12 de marzo de 2018, un total de capitalización de mercado de \$347,812,342,837 dólares.

De este total de criptomonedas, las 10 mejores son: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Cardano, NEO, Stellar, Monero y Dash. Al 12 de marzo de 2018 la capitalización de mercado de Bitcoin fue de \$157,676.04 millones de dólares, con un precio de \$9,321.6 dólares, y un total de 16.9 millones de acciones en circulación. El segundo lugar lo ocupó Ethereum con un total de 98.1 millones de acciones en circulación y una capitalización de mercado de \$69,111.9 millones de dólares; el costo de cada ether fue de \$704.19 dólares.

El tercer lugar lo ocupó Ripple con una capitalización de mercado de \$31,456.1 millones de dólares y tuvo un costo de \$0.8047 dólares. Bitcoin Cash se mantuvo en cuarto lugar con una capitalización de mercado de \$17,957.1 millones de dólares y un total de 17.01 millones de acciones en circulación, seguido por Litecoin, que obtuvo una capitalización de mercado de \$10,066.8 millones de dólares y un precio de \$181 dólares, con un total de 55.5 millones de acciones en circulación.

Cardano permaneció en sexto lugar del top ten, con un total de 25,027.07 millones de acciones en circulación y un total de capitalización de mercado de \$5,777.5 millones de dólares. NEO tuvo una capitalización de mercado de \$5.630.9 millones de dólares, un precio de \$86.6 dólares y un total de 65 millones de acciones en circulación.

Fuente: Tomado de CoinMarketCap, *Capitalización de mercado de criptomoneda*, última actualización el 12 de marzo de 2018, disponible en <https://coinmarketcap.com> (fecha de consulta: febrero de 2018).

En el noveno lugar se encontró a Monero, con un total de 15.8 millones de acciones en circulación, una capitalización de mercado total de \$4,198.2 millones de dólares. El último lugar es para Dash, con una capitalización de mercado de \$4,093.8 millones de dólares y un total de 7.9 millones de acciones en circulación.

### Las mejores 10 criptomonedas (dólares)

#	Nombre	Símbolo	Capital de mercado	Precio	Acciones en circulación
1	Bitcoin	BTC	\$ 157,676,048,050	\$ 9,321.6700	16,915,000
2	Ethereum	ETH	\$ 69,111,995,135	\$ 704.1900	98,143,402
3	Ripple	XRP*	\$ 31,456,124,803	\$ 0.8047	39,091,956,706
4	Bitcoin Cash	BCH	\$ 17,957,109,665	\$ 1,055.4500	17,013,700
5	Litecoin	LTC	\$ 10,066,817,476	\$ 181.0700	55,595,968
6	Cardano	ADA*	\$ 5,777,588,399	\$ 0.2228	25,927,070,538
7	NEO	NEO*	\$ 5,630,995,500	\$ 86.6300	65,000,000
8	Stellar	XLM*	\$ 5,440,389,155	\$ 0.2941	18,498,433,032
9	Monero	XMR	\$ 4,198,268,085	\$ 265.4400	15,816,320
10	Dash	DASH	\$ 4,093,882,355	\$ 515.4900	7,941,745

\*No minable.

Fuente: Tomado de CoinMarketCap, *Capitalización de mercado de criptomoneda*, última actualización el 12 de marzo de 2018, disponible en <https://coinmarketcap.com> (fecha de consulta: febrero de 2018).



# 4. Plataformas de Bitcoin del mercado

Desde que Bitcoin comenzó a popularizarse se creó en torno a esta criptomoneda un amplio, pero también inestable, ecosistema de aplicaciones, plataformas, servicios para gestionar el almacenamiento y las transacciones en esta moneda. Entre las más importantes se encuentran:

### ➤ **BitPay**

Es el mayor proveedor de servicios de pago con bitcoin a nivel mundial. Fue fundada en 2011 por Anthony Gallippi y Stephen Pair (presidente y CEO de la compañía). Tiene su sede en Atlanta. En 2014 abrió oficinas en Nueva York, San Francisco, Ámsterdam y Buenos Aires.

Su alianza con Automattic para implementar los pagos con bitcoin en Wordpress.com fue el primer espaldarazo público de una compañía tecnológica a la nueva moneda digital, iniciando así una tendencia lenta pero imparable desde entonces. Con su pasarela de pago para WooCommerce (el plugin de e-commerce para WordPress) abrió las puertas de cientos de miles de tiendas online al bitcoin. En ese momento BitPay ya gestionaba mensualmente transacciones por un valor medio de cinco millones de dólares.

En 2013 BitPay promovió la creación de una fundación para impulsar las donaciones caritativas en bitcoins: BitGive. Ha establecido alianzas con Save the Children y ha recaudado casi 5,000 euros en un solo día para las víctimas de un tifón en Filipinas.

### ➤ **Coinbase**

Esta plataforma nació en 2012 en San Francisco. Su pretensión era proveer a los usuarios con un perfil poco técnico de una herramienta con la cual poder gestionar de forma sencilla sus bitcoins, al tiempo que proporcionaban a las empresas servicios de pago online.

Fuente: Tomado de BBVA, *Las principales plataformas de bitcoin del mercado*, 30 de enero de 2015, disponible en [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).

En 2014, Coinbase había recibido 31 millones de dólares en inversiones de empresas de capital riesgo como Andreessen Horowitz y Union Square Ventures; a lo largo de ese año se convirtió en el procesador de pagos de sitios webs de gran relevancia como Expedia, Overstock, Wikipedia, Dell y Time. En 2015, Coinbase anunció la creación de Coinbase Exchange, la primera entidad financiera regulada con el fin de realizar cambios entre dólares americanos y bitcoins, con capacidad para operar en la mitad de los estados de Estados Unidos, entre ellos Nueva York y California. Empezó a operar el 30 de marzo de 2015.

### ➤ **GoCoin**

Esta plataforma, construida sobre la base de un software programado en lenguaje Go y publicado en mayo de 2013, destaca por trabajar también con Litecoin y Dogecoin. Al día de hoy mantiene acuerdos con plataformas como Cozy Games (de juegos de azar online) y Shopify (CMS para e-commerce).

Fuente: Tomado de BBVA, *Las principales plataformas de bitcoin del mercado*, 30 de enero de 2015, disponible en [www.bbva.com](http://www.bbva.com) (fecha de consulta: febrero de 2018).



# 5. Regulación de criptomonedas en México

El 1 de marzo de 2018 se aprobó el Proyecto de decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera. Esta nueva legislación coloca a México a la vanguardia a nivel internacional en materia de regulación de servicios financieros, ya que establece las herramientas regulatorias necesarias para el sano desarrollo de este sector. Con esta nueva legislación se crean dos nuevos tipos de entidades financieras que son: las Instituciones de Financiamiento Colectivo y las Instituciones de Fondos de Pago Electrónico, y establece la posibilidad de que se establezcan modelos electrónicos novedosos para la prestación de servicios financieros por entidades financieras y por terceros.

Minuta	Turno a comisión	Sinopsis	Proceso legislativo
<p>Proyecto de decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman, adicionan y derogan diversas disposiciones de la Ley de Instituciones de Crédito, la Ley del Mercado de Valores, la Ley General de Organizaciones y Actividades Auxiliares del Crédito, la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, la Ley para Regular las Sociedades de Información Crediticia, la Ley de Protección y Defensa al Usuario de Servicios Financieros, la Ley para Regular las Agrupaciones Financieras, la Ley de la Comisión Nacional Bancaria y de Valores, y la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.</p> <p><b>Proponente:</b> Minutas  <b>Fecha de presentación:</b> 7-diciembre-2017  <b>Cámara de Origen:</b> Cámara de Diputados</p>	<p>Hacienda y Crédito Público  publicación en Gaceta: 7-diciembre-2017</p>	<p>Contar con un ordenamiento jurídico que tenga por objeto regular los servicios financieros que prestan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento y los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores; con base en los principios de inclusión e innovación financiera, promoción de la competencia, protección al consumidor, preservación de la estabilidad financiera, prevención de operaciones ilícitas y neutralidad tecnológica.</p>	<p>Estado actual:  Aprobada  con fecha 1-marzo-2018</p> <p>Proceso Legislativo:  1. Iniciativa enviada a la Cámara de Senadores por el Ejecutivo federal el 9 de octubre de 2017.  2. Dictamen a discusión presentado en la Cámara de Senadores el 5 de diciembre de 2017. Proyecto de decreto aprobado por 104 votos.  3. Pasa a la Cámara de Diputados para los efectos del apartado A) del artículo 72 de la CPEUM.  4. Minuta recibida en la Cámara de Diputados el 7 de diciembre de 2017.  5. Dictamen a discusión presentado en la Cámara de Diputados, el 1 de marzo de 2018. Proyecto de decreto aprobado en lo general y en lo particular, los artículos no reservados por 286 votos a favor, 3 en contra y 63 abstenciones.  6. Pasa al Ejecutivo federal para sus efectos constitucionales.</p>

Fuente: Tomado de la Cámara de Diputados, *Minutas presentadas en la LXIII Legislatura turnadas a comisión*, disponible en <http://sitl.diputados.gob.mx> (fecha de consulta: marzo de 2018).



# CENTRO DE ESTUDIOS SOCIALES Y DE OPINIÓN PÚBLICA



CÁMARA DE DIPUTADOS  
LXIII LEGISLATURA

[diputados.gob.mx/cesop](http://diputados.gob.mx/cesop)

 [cesop01](https://www.facebook.com/cesop01)

 [@cesopmx](https://twitter.com/cesopmx)

Responsable de la publicación: Lic. Karen Nallely Tenorio Colón