Grant Thornton

Boletín informativo

Noviembre 2025-03

Un viaje al mundo mágico del dinero digital: ¿Qué son las Criptomonedas?

En el mundo, existen dos tipos de dinero. Está el dinero que se puede tocar: las monedas que suenan en el bolsillo y los billetes que se guardan en una cartera. Pero también hay otro tipo de dinero, uno que vive dentro de las computadoras y los teléfonos. Es un dinero digital.

Para entenderlo, se puede pensar en las monedas o gemas que se coleccionan en un videojuego. No se pueden sostener en la mano, pero se trabaja duro para conseguirlas, y se pueden usar para comprar objetos increíbles dentro del juego. Esas monedas digitales tienen un valor real en ese mundo virtual. Ahora, ¿qué pasaría si se pudieran usar esas mismas monedas del juego para comprar cosas en el mundo real, como un juguete o un helado? Esa es la idea fundamental detrás de las criptomonedas: un dinero que vive dentro de las computadoras pero que tiene un valor verdadero en nuestro mundo.

Antes de que existieran las criptomonedas, enviar dinero por internet siempre requería la ayuda de un adulto en el medio, como un banco. Si una persona quería enviar dinero a un amigo que vivía en otra ciudad, tenía que pedirle al banco que lo hiciera. Esto es como pedirle a un profesor que supervise cada intercambio de cromos en el patio del colegio. El proceso es lento, y el profesor siempre está a cargo, tomando nota de todo. Las criptomonedas se inventaron para que los amigos pudieran intercambiar valor directamente entre ellos, sin importar en qué parte del mundo se encuentren, sin necesidad de que un banco o un profesor esté en medio. Es una forma de tener dinero que pertenece completamente a las personas que lo usan.

El nacimiento de una idea secreta

a) Su origen

La historia de las criptomonedas comienza con un gran misterio. En el año 2008, una persona o un grupo de personas, usando el nombre secreto de Satoshi Nakamoto, tuvo una idea revolucionaria. Nadie sabe quién es Satoshi en realidad; es como un superhéroe cuya verdadera identidad permanece oculta. El 31 de octubre de 2008, Satoshi envió un mensaje a una lista de correo de expertos en códigos y secretos (criptografía), describiendo un "nuevo sistema de efectivo electrónico" al que llamó Bitcoin. Su objetivo era muy ambicioso: crear un medio de pago que fuera rápido, barato y, lo más importante, que no pudiera ser controlado por ningún gobierno o banco del mundo.

El 3 de enero de 2009, Satoshi Nakamoto puso en marcha la red Bitcoin. Lo hizo creando el primer conjunto de transacciones, conocido como el "Bloque Génesis". Fue como escribir la primera página de un cuaderno nuevo y completamente vacío. Dentro de este primer bloque, Satoshi escondió un mensaje secreto, el titular de un periódico de ese día: "The Times Jan 3, 2009 Chancellor on brink of second bailout for banks" (Canciller al borde de un segundo rescate para los bancos). Este mensaje era una pista sobre la razón de ser de Bitcoin: ofrecer una alternativa al sistema bancario tradicional, que en aquel momento enfrentaba serios problemas. La decisión de Satoshi de permanecer en el anonimato fue fundamental. Si su identidad fuera conocida, la gente lo vería como el líder de Bitcoin, y los gobiernos podrían presionarlo. Esto crearía un punto central de control, justo lo que Bitcoin fue diseñado para evitar. Al desaparecer, Satoshi se aseguró de que la comunidad tuviera que aprender a gestionar el sistema por sí misma, manteniendo su naturaleza verdaderamente descentralizada y sin un líder visible.

Al principio, Bitcoin era solo un pasatiempo para expertos en computación y no tenía casi ningún valor. La primera cotización registrada fue de apenas 0,00076 dólares por un bitcoin. El momento que lo cambió todo llegó el 22 de mayo de 2010, un día que ahora se celebra como el "Bitcoin Pizza Day". Un programador llamado Laszlo Hanyecz ofreció pagar 10.000 bitcoins a quien le llevara dos pizzas a su casa. Alguien aceptó el trato, y Laszlo recibió sus pizzas a cambio del dinero digital. En ese momento, esos 10.000 bitcoins valían unos 41 dólares. Este evento fue histórico porque demostró por primera vez que este "dinero de internet" podía usarse para comprar algo real y tangible. Fue el puente psicológico que conectó un concepto digital abstracto con la economía física. Permitió que personas fuera del círculo de expertos entendieran que Bitcoin podía funcionar como dinero, lo que despertó el interés y la demanda, haciendo que su valor comenzara a crecer. Esas mismas 10.000 monedas que compraron dos pizzas llegarían a valer cientos de millones de dólares años después.

El cuaderno mágico que nadie puede borrar

b) Que es el blockchain

Para entender cómo funcionan las criptomonedas, es necesario imaginar un cuaderno muy especial, un cuaderno mágico. Supongamos que un grupo de amigos tiene un club y quieren llevar la cuenta de sus intercambios de juguetes. En lugar de que una sola persona guarde el cuaderno, lo cual sería arriesgado si lo pierde o hace trampa, cada miembro del club recibe una copia idéntica del mismo cuaderno. Este cuaderno compartido es la *blockchain*, también conocida como "cadena de bloques". En el mundo de la tecnología, a esto se le llama un "libro de contabilidad distribuido".

Este cuaderno mágico tiene reglas muy estrictas que lo h acen increíblemente seguro. Cada página del cuaderno se llama "bloque", y en cada bloque se anota una lista de las transacciones más recientes, como "Ana le dio una canica a Carlos" o "Pepe le dio un bitcoin a Chuchito". Cuando una página (un bloque) se llena de anotaciones, se añade al cuaderno. Aquí es donde ocurre la magia: cada nueva página se une a la página anterior con un código secreto súper fuerte y único, llamado *hash*. Este código se crea a partir de toda la información de la página anterior. De esta manera, las páginas forman una cadena irrompible: una "cadena de bloques" o *blockchain*.

La seguridad de este sistema es asombrosa. Como cada bloque está matemáticamente encadenado al anterior, es imposible alterar una página antigua sin ser descubierto. Si alguien intentara cambiar una anotación en la página 5, el código secreto que la une a la página 6 se rompería. Inmediatamente, las copias del cuaderno de todos los demás miembros del club mostrarían que esa cadena está rota, y sabrían que alguien ha intentado hacer trampa. Esta característica hace que la blockchain sea "inmutable", lo que significa que una vez que algo se escribe, no se puede cambiar ni borrar.

La consecuencia más importante de este diseño es que no se necesita un jefe. Como todos los participantes tienen una copia del cuaderno y pueden verificar que las reglas se están cumpliendo, no hace falta un banco o una autoridad central que supervise todo. La confianza no se deposita en una persona o una empresa, sino en el propio sistema: en las matemáticas y el código que son visibles para todos. A esto se le llama "descentralización". Los ordenadores que forman parte de esta red se llaman "nodos", y todos colaboran para mantener la exactitud del cuaderno mágico. En esencia, la verdadera innovación de la blockchain no es solo una nueva forma de almacenar datos, sino una manera de generar confianza entre desconocidos sin necesidad de un intermediario. Permite que dos personas que nunca se han visto puedan intercambiar valor con la misma seguridad que si un banco estuviera supervisando la operación. Además, como la información está copiada en miles de ordenadores por todo el mundo, la red es increíblemente resistente. No hay un servidor central que un gobierno pueda apagar o un hacker pueda atacar, lo que la hace no solo robusta, sino también una herramienta poderosa para la libertad financiera.

Los guardianes del cuaderno

c) Que es la minería

Si todos tienen una copia del cuaderno, surge una pregunta importante: ¿quién tiene el permiso para escribir las nuevas páginas y añadirlas a la cadena? La respuesta es: unos participantes muy especiales llamados "mineros". Pero estos mineros no usan cascos ni picos. En su lugar, utilizan ordenadores extremadamente potentes, diseñados específicamente para una tarea muy difícil. Su trabajo es ser los guardianes y escribanos de la blockchain.

Los mineros tienen dos misiones principales. La primera es actuar como detectives. Recopilan todas las nuevas transacciones que la gente quiere realizar y las revisan cuidadosamente para asegurarse de que son legítimas. Verifican, por ejemplo, que nadie esté intentando gastar el mismo dinero dos veces, un tipo de trampa conocido como "doble gasto". Una vez que han reunido un grupo de transacciones válidas, las preparan para formar un nuevo bloque.

La segunda misión es la más desafiante: para ganarse el derecho de añadir ese nuevo bloque a la cadena, todos los mineros del mundo compiten entre sí para ser el primero en resolver un acertijo matemático increíblemente complejo. Este acertijo no requiere ser un genio de las matemáticas, sino tener un ordenador capaz de hacer billones de intentos por segundo, probando combinaciones al azar hasta dar con la solución correcta. Este proceso de competencia se llama "Prueba de Trabajo" (*Proof-of-Work*), porque el ganador debe demostrar que su ordenador ha realizado una enorme cantidad de trabajo para encontrar la respuesta.

El primer minero cuyo ordenador resuelve el acertijo gana un premio muy valioso. Recibe dos cosas: primero, una "recompensa por bloque", que consiste en una cantidad de criptomonedas completamente nuevas, recién creadas. Así es como nacen los nuevos bitcoins y entran en circulación. Segundo, también se queda con las pequeñas comisiones que los usuarios añadieron a sus transacciones para que fueran procesadas.

Este sistema de minería es mucho más que un juego. Cumple dos funciones vitales: es el método por el cual las nuevas transacciones se añaden de forma segura a la blockchain y es la única manera de crear nuevas monedas. El sistema está diseñado de tal manera que el interés propio de cada minero (ganar la recompensa) contribuye directamente a la seguridad y el bien común de toda la red. Para hacer trampa, un actor malintencionado necesitaría controlar más de la mitad de toda la potencia informática de la red, lo que requeriría una inversión gigantesca en equipos y electricidad, haciendo que el ataque sea económicamente inviable. Además, el sistema tiene un mecanismo de ajuste automático: la dificultad del acertijo cambia aproximadamente cada dos semanas para asegurar que, sin importar cuántos mineros estén compitiendo, un nuevo bloque se añada siempre cada diez minutos. Esta genialidad oculta garantiza que la creación de nuevas monedas sea constante y predecible, un pilar fundamental de su modelo económico.

¿Por qué vale algo un tesoro digital?

d) Cuál es el respaldo de la criptomoneda

Una de las preguntas más comunes sobre las criptomonedas es: si no están hechas de oro y ningún gobierno las respalda, ¿por qué valen algo? El dinero tradicional, como los dólares o los euros, tiene valor porque los gobiernos decretan que es de curso legal y la gente confía en esa promesa. Las criptomonedas, en cambio, no tienen este tipo de respaldo oficial. Su valor proviene de otras fuentes, de forma muy parecida a como un cromo raro o una obra de arte adquieren su valor. No es el material del que están hechos lo que importa, sino lo que la gente piensa de ellos.

El valor de una criptomoneda se basa en tres ingredientes mágicos principales:

1. **Confianza y acuerdo (Comunidad):** El factor más importante es que una gran comunidad de personas en todo el mundo cree que tiene valor y está dispuesta a aceptarla como forma de pago. Si millones de personas desean algo y lo utilizan para intercambiar bienes y servicios, ese algo se vuelve valioso por consenso. Es un valor que nace del acuerdo colectivo.
2. **Utilidad (Uso práctico):** Las criptomonedas son útiles. Permiten enviar valor a cualquier parte del mundo en cuestión de minutos, sin necesidad de un banco como intermediario y, a menudo, con comisiones más bajas que los sistemas tradicionales. Otorgan a las personas un control total

sobre su propio dinero, sin que nadie pueda congelarlo o confiscarlo sin su permiso. Las cosas que resuelven problemas reales y ofrecen ventajas tienden a ser valiosas.

3. **Escasez (Rareza):** Este es un pilar fundamental. Las reglas de muchas criptomonedas, y en especial de Bitcoin, establecen que solo existirá un número limitado de monedas. En el caso de Bitcoin, el límite máximo es de 21 millones. Una vez que todas las monedas hayan sido "minadas" (lo que se estima ocurrirá alrededor del año 2140), no se podrán crear más. Esta escasez programada es similar a la de los metales preciosos como el oro o los diamantes. Las cosas que son útiles y, al mismo tiempo, raras, tienden a mantener o aumentar su valor con el tiempo. Esto contrasta fuertemente con el dinero tradicional, que los gobiernos pueden imprimir en cantidades ilimitadas, haciendo que con el tiempo pierda valor.

Para visualizar mejor estas diferencias, la siguiente tabla compara el dinero que usamos todos los días con el dinero digital.

Tabla: Dinero de bolsillo vs. dinero digital

Característica	Dinero normal (Euros, Dólares)	Criptomoneda (Bitcoin)
¿Quién lo crea?	Un gobierno y su banco central.	Un programa de computadora y los "mineros".
¿Quién lo controla?	Los bancos y el gobierno.	Nadie y todos. La comunidad de usuarios.
¿Es físico?	Sí, tienes monedas y billetes.	No, solo existe en las computadoras.
¿Por qué vale?	Porque el gobierno dice que vale.	Porque la gente confía en él, lo usa y es escaso.
¿Cómo se envía?	Se lo das a alguien o usas un banco.	Lo envías por internet, de persona a persona.

El sube y baja de los precios

e) Cuál o cómo se determina el valor de la criptomoneda y de su valor razonable

El precio de una criptomoneda se decide de una manera muy parecida a como se decide el valor de los cromos en el patio del colegio: todo se reduce a la ley de la **oferta y la demanda**. No hay un precio oficial fijado por una autoridad; su valor es simplemente lo que la gente está dispuesta a pagar por él en un momento dado en el mercado.

Los dos conceptos clave son:

- **Oferta:** Se refiere a cuántas monedas de una criptomoneda están disponibles para la venta. Como ya se ha visto, en el caso de Bitcoin, la oferta total es limitada y conocida.
- **Demanda:** Se refiere a cuántas personas quieren comprar esa criptomoneda en un momento determinado.

El mecanismo funciona de la siguiente manera: si una noticia positiva o el entusiasmo general hacen que mucha gente quiera comprar una criptomoneda (alta demanda), pero la cantidad disponible para la venta es limitada (baja oferta), los compradores estarán dispuestos a pagar más para conseguirla. Como resultado, el precio sube. Por el contrario, si surgen noticias negativas o la gente pierde el interés (baja demanda) y muchos deciden vender sus monedas (alta oferta), el precio caerá porque los vendedores tendrán que bajarlo para encontrar compradores.

Esta dinámica explica por qué los precios de las criptomonedas pueden cambiar tan rápidamente. Este fenómeno se conoce como "volatilidad". A diferencia de activos tradicionales como las acciones de una empresa, cuyo valor se puede estimar en función de sus beneficios futuros, las criptomonedas no generan ingresos por sí mismas. Su valor está impulsado en gran medida por la especulación y el sentimiento del mercado: lo que la gente *cree* que valdrá en el futuro. Esto hace que su precio sea muy sensible a las noticias, las tendencias en redes sociales y la psicología de los inversores.

Además, la escasez programada de Bitcoin le confiere una característica económica muy particular. Mientras que el dinero tradicional es "inflacionario" (los gobiernos imprimen más, y cada unidad vale un poco menos con el tiempo), Bitcoin es "deflacionario". Como su oferta es fija, si la demanda sigue creciendo a largo plazo, es lógico pensar que su valor por unidad también lo hará. Esta expectativa incentiva a muchas personas a comprar Bitcoin no para gastarlo inmediatamente, sino para guardarlo como una inversión o una "reserva de valor", similar al oro digital, con la esperanza de que su valor aumente en el futuro.

¿Quién cuida y juega con las Criptomonedas?

f) Quién es el que mantiene y negocia el "inventario" de criptomonedas

Una de las ideas más difíciles de entender sobre las criptomonedas es que no hay una empresa, un director o un presidente a cargo. No existe "Bitcoin, S.A.". La red se mantiene viva y funcional gracias a la colaboración de un equipo global y descentralizado, donde diferentes grupos de personas desempeñan roles distintos, pero igualmente importantes. Es un sistema de gobierno con controles y equilibrios, similar al de un país.

Los tres grupos principales que mantienen la red son:

1. **Los mineros:** Como ya se ha explicado, son los guardianes que aportan la potencia de sus ordenadores para validar transacciones y construir la blockchain. Son como el poder ejecutivo: ejecutan las reglas del sistema y mantienen su funcionamiento diario a cambio de una recompensa económica.
2. **Los nodos:** Un "nodo" es cualquier ordenador en el mundo que descarga y mantiene una copia completa y actualizada de toda la historia de la blockchain. Su función es crucial: actúan como los árbitros o el poder judicial de la red. Verifican de forma independiente cada transacción y cada bloque, asegurándose de que los mineros sigan las reglas al pie de la letra. Miles de voluntarios operan nodos, y su poder colectivo garantiza que nadie pueda cambiar las reglas del sistema sin el acuerdo de la mayoría.
3. **Los desarrolladores:** Son los programadores y expertos en software que trabajan para mejorar el código de Bitcoin. Son como el poder legislativo: proponen nuevas leyes (actualizaciones de software) para corregir errores o añadir nuevas funcionalidades. Sin embargo, no pueden imponer estos cambios. Para que una actualización se implemente, debe ser aceptada voluntariamente por la gran mayoría de los nodos de la red. Este equilibrio de poder entre desarrolladores, mineros y nodos es lo que protege a la red de ser controlada por un solo grupo.

En cuanto a dónde se negocia el "inventario" de criptomonedas, la gente no acude a un banco tradicional. En su lugar, utilizan plataformas en línea llamadas **Exchanges** (casas de cambio). Un exchange es un mercado digital donde las personas pueden comprar, vender e intercambiar criptomonedas usando dinero tradicional (como euros o dólares) u otras criptomonedas. Plataformas como Coinbase, Binance o Bit2Me son algunos de los exchanges más conocidos. Es en estos mercados donde la oferta y la demanda se encuentran y se determina el precio en tiempo real.

Una vez que se compra una criptomoneda, se almacena en un **"monedero" o "billetera" digital** (*wallet*). Este es un programa o dispositivo que guarda las claves secretas que dan acceso a los fondos, funcionando como una cuenta bancaria personal de la que solo el propietario tiene el control. Aquí surge una paradoja interesante: aunque Bitcoin es un sistema descentralizado, la forma más fácil de acceder a él es a través de estos exchanges, que son empresas centralizadas. Esto reintroduce un intermediario de confianza, exponiendo a los usuarios a riesgos como hackeos o la intervención de gobiernos, precisamente los problemas que Bitcoin fue diseñado para resolver.

El futuro del dinero de Internet

El viaje por el mundo de las criptomonedas revela una idea tan simple como poderosa: un dinero digital que no necesita jefes. Nació de la mente misteriosa de Satoshi Nakamoto con la promesa de un sistema financiero más abierto y justo. Su funcionamiento se basa en una tecnología ingeniosa llamada blockchain, un cuaderno de cuentas mágico, compartido y a prueba de trampas, que es protegido por una comunidad global de "mineros".

Se ha aprendido que su valor no proviene del oro ni de un decreto gubernamental, sino de la confianza de las personas que lo usan, de su utilidad para mover valor por el mundo y de su escasez, que lo asemeja a un tesoro digital. Su precio sube y baja según el entusiasmo y el interés del mercado, en un constante baile de oferta y demanda.

El mundo de las criptomonedas es todavía joven y está en plena evolución. Es como eran los primeros días de internet: un territorio nuevo, lleno de posibilidades y desafíos. Nadie sabe con certeza cómo será el futuro, pero esta tecnología ya ha demostrado que es posible imaginar el dinero de una forma diferente: un dinero global, transparente y que, en última instancia, pertenece a todos los que participan en él. La aventura no ha hecho más que empezar.

Cómo podemos ayudarle

Esperamos que la información le resulte útil. Si desea ampliar cualquiera de los puntos planteados, contacte con grantthornton.com.ve

Jorge Gómez C.
Socio
E grant.thornton@ve.gt.com

Karly Terán
Gerente de Auditoría
E grant.thornton@ve.gt.com