Guía práctica de conceptos claves sobre criptomonedas

Beaudroit, Manuel

Abstract: La idea del presente artículo es, con base en los conocimientos técnicos del autor como especialista en la materia, brindarles a los profesionales una guía práctica sobre los conceptos claves de las criptomonedas.

I. ¿Que son las criptomonedas?

Una criptomoneda es un tipo de dinero digital que usa criptografía para dar seguridad a sus transacciones, así como gestionar su emisión y asegurar su propiedad. Una característica fundamental de las criptomonedas es que no son emitidas ni controladas por autoridades centrales de ningún tipo, ya sea trate de estados o de empresas.

Desde que la digitalización impactó múltiples áreas de nuestras vidas, el dinero no fue la excepción. Tarjetas de débito, transferencias bancarias y muchas otras implementaciones de tecnología permitieron librarse del papel y simplificaron en gran medida la forma en que las personas transaccionamos en nuestro día a día.

Sin embargo, hasta el momento no había sido posible utilizar dinero sin que una institución de tipo centralizado canalice las operaciones y evite actos maliciosos. Ya sea a través de un banco, una empresa emisora de tarjetas, o un Estado por medio de un Banco Central, el dinero digital circuló siempre con intermediación de terceros, en los cuales las personas se ven obligadas a depositar su confianza.

¿Como se asegura, por ejemplo, que no exista una duplicación o falsificación de la moneda digital —fenómeno también conocido como "doble gasto"—? Hasta el año 2008, la respuesta era única: a través de un intermediario que garantice la disponibilidad de esos fondos en la cuenta de quien los envía.

La aparición de bitcoin crea un nuevo paradigma. La primera criptomoneda nace con una naturaleza descentralizada y prescinde de todo intermediario. Se trata de un sistema libre y transparente, resistente a la censura y que no conoce de fronteras ni jurisdicciones.

Las criptomonedas forman parte de una revolución en curso y prometen transformar muchas de las concepciones que tenemos acerca del valor y del dinero, fundamentalmente, además de impactar en muchos otros ámbitos de nuestras vidas.

II. ¿Cómo funcionan las criptomonedas?

Existen miles de criptomonedas, por lo que es difícil definir cómo funcionan las cripto en general. Los casos de uso son variados, así como su nivel de descentralización y autonomía.

Sí es posible detenerse en los puntos en común que comparten la mayoría de las criptomonedas y que hace a su esencia: la utilización de tecnología blockchain para el registro de las transacciones y la toma de decisiones a partir del consenso distribuido de las partes de una misma red.

Una especie de base de datos descentralizada y pública conocida como cadena de bloques (o blockchain) permite registrar todas las transacciones que ocurren de una criptomoneda. Se incorpora una huella de tiempo a cada una de ellas, dando a la totalidad del registro una característica clave: la información es inmutable, no puede modificarse ni eliminarse.

¿Quién valida las operaciones? El consenso de los propios nodos de la red. La gobernanza del sistema está distribuida entre ellos, cada uno de los cuales almacena una copia completa de la cadena de bloques e incorpora las nuevas transacciones a medida que ocurren, dando fe

de su validez y evitando que puedan existir duplicaciones o falsificaciones.

El modo en que los nodos de la red validan transacciones puede variar según la criptomoneda de la que se trate. Lo que no es variable es la necesidad de un algoritmo de consenso que se da entre los usuarios de esa red.

El consenso distribuido distingue a las criptomonedas de cualquier moneda digital controlada por una o pocas entidades. A la vez, es el elemento que permite evitar vulnerabilidades y ataques: todos los nodos almacenan una copia de la cadena, por lo que la información permanece segura en caso de que uno de ellos sufra un hackeo.

¿Por qué cripto? Porque es la tecnología criptográfica la que se utiliza para asegurar las transacciones, controlar la emisión de nuevas unidades y verificar su propiedad.

III. Diferentes criptomonedas

Desde el nacimiento de Bitcoin en 2008, nuevos desarrollos se han sucedido, con un sinnúmero de proyectos que emergieron y propusieron soluciones a distintos problemas a partir de la utilización de la tecnología blockchain. Nuevas monedas, tokens con distintos casos de uso adquirieron valor a raíz de su intercambio.

IV. Cada criptomoneda podría pensarse como una propuesta de solución a un problema determinado

El nacimiento de bitcoin, por ejemplo, se encuentra ligado al interés por crear un medio de pago altamente seguro, una forma de transferir valor sin intermediarios. A diferencia de las monedas fiduciarias que predominaban en el mundo de aquel entonces y de hoy, bitcoin es eminentemente escaso: su emisión nunca crecerá por encima de una magnitud establecida de antemano, lo cual constituye una fortaleza.

La aplicación monetaria fue el primer caso de uso popularizado para la tecnología blockchain, pero de ninguna manera es el único. En 2014 nace Ethereum.

Ethereum permite ejecutar contratos inteligentes (smart contracts) sobre una blockchain pública. Los smart contracts consisten en contratos entre partes establecidos en código computacional que se ejecutan de forma confiable, sin terceros intermediarios, tras cumplirse condiciones establecidas de antemano.

Ahora es posible gracias a Ethereum desarrollar aplicaciones descentralizadas, que no residen en un único servidor sino en una blockchain pública. Las posibilidades son variadas: desde alojar a múltiples aplicaciones que hoy se desarrollan en la web centralizada, hasta migrar muchos otros procesos que hoy se realizan en el mundo físico y requieren de confianza o intermediarios para su concreción

Ether (ETH) es la criptomoneda utilizada para pagar los costos de operar en la red. Naturalmente, la utilización de la plataforma y la especulación en torno al potencial que tiene la red elevaron el interés por su token, que hoy se ubica solo detrás de bitcoin en capitalización de mercado.

Como Ethereum, el potencial de las aplicaciones descentralizadas (DApps) gracias a la utilización de smart contracts motivó el desarrollo de distintas plataformas que comparten su propósito, pero incorporan modificaciones de forma o de fondo. La mayoría de ellas tienen a su vez un token nativo, utilizado para el pago de las comisiones de red.

Así, Binance Smart Chain dio origen al token BNB, Cardano al token ADA, Polygon a MATIC, Polkadot a DOT, Solana a SOL, y muchas otras más que coexisten y buscan dar respuesta a un problema planteado.

Sin embargo, los casos de uso de criptomonedas no acaban ahí. Hay tokens que funcionan

mayoritaria —y a veces exclusivamente— para la gobernanza de un sistema. Usualmente, a través de la posesión de un token los usuarios acceden a tomar decisiones y votar en torno a propuestas. Se trata de un esquema de incentivos que busca alinear los intereses de una organización y sus miembros a la vez, resolviendo el problema de coordinación ante la ausencia de autoridad o estructura jerárquica.

Un ejemplo es el del token MKR, que permite ejercer la gobernanza del protocolo Maker. Los poseedores del token pueden tomar decisiones relevantes en torno al sistema, cómo el nivel de colateral necesario para emitir DAI, una criptomoneda estable atada al precio del dólar.

Con criptomoneda estable (o stablecoin) se hace referencia a toda aquella cripto que está atada al precio de otra moneda o activo. Al mantener un precio estable, resulta ideal para quienes prefieren no exponerse a la volatilidad del resto de las criptomonedas. Lo más común es que tengan una paridad fija con el dólar estadounidense, aunque no es excluyente y las hay de distintos tipos.

Las más conocidas son Tether (USDT), DAI y USD Coin (USDC)

V. ¿Qué tipo de monederos digitales existen?

Existen distintos tipos de billetera para interactuar con tu saldo de criptomonedas, enviar y recibir fondos y almacenar tus llaves privadas de acceso.

Según el criterio utilizado, distinguimos:

- Billeteras custodial y non-custodial.

- Billeteras virtuales y físicas.

- Billeteras calientes y frías.

Es importante tener en cuenta cómo funciona una billetera o monedero. A diferencia del concepto más común, no almacenan criptomonedas: una billetera almacena las herramientas necesarias para interactuar con la cadena de bloques.

Para ejecutar una operación en una blockchain, como Bitcoin, es necesario no solo disponer de una "llave pública" que identifica al monedero y permite generar direcciones para el envío, sino de una "llave privada" que solamente posee quien tiene los fondos en su propiedad.

En un banco tradicional existe un número de cuenta al que pueden enviarse fondos, y a la vez datos de inicio de sesión, como un PIN, para que su poseedor pueda interactuar con el saldo que ha depositado en el banco. En este caso el funcionamiento es similar.

Así como la llave privada es la que te garantiza la propiedad y el acceso a tus criptomonedas, resguardar o no esa llave es lo que distinguirá a una custodial de una non-custodial (o self-custodial) wallet.

Mientras que una billetera custodial mantiene la llave privada resguardada por un tercero y brinda una interfaz simple para acceder al manejo de los saldos, una billetera non custodial permite mantener al usuario la custodia de su llave privada, y por ende el total control de sus fondos.

Un monedero puede ser de tipo virtual o físico, poniendo cada formato el foco en una u otra cualidad.

Por un lado, un software que hace posible la visualización e interacción con tu saldo de criptomonedas a través de una interfaz simple, que puede o no resguardar tus llaves. Puede tratarse de una billetera para usar en dispositivos móviles, como extensión en navegadores web, o como aplicación de escritorio.

Por otro lado, los monederos físicos (o hardware wallets) ofrecen la posibilidad de almacenar las claves en un dispositivo desconectado de internet. Suelen ser preferidos por los usuarios que almacenan a largo plazo sus saldos y buscan priorizar la seguridad.

Las billeteras virtuales y físicas están muy relacionadas al último criterio.

En ese caso, la diferencia consiste en la conexión o desconexión de internet. Una billetera caliente (o hot wallet) es aquella que de algún modo está conectada a internet. Se puede acceder a los fondos fácilmente por lo que son usadas por los usuarios frecuentes.

Una billetera fría (o cold wallet) no se encuentra conectada a internet. Es preferida para el almacenamiento "en frío" de los saldos, priorizando el resguardo de las llaves privadas ante posibles ataques o vulnerabilidades.

VI. ¿Cómo se determina su valor?

Como en todo mercado libre, sin restricciones a la entrada y salida, el valor que adquiera una criptomoneda será reflejo de las variaciones que existan en su oferta y demanda.

Los juicios y valoraciones que las personas hacen sobre un bien, servicio o activo financiero pueden ser sumamente variables. Estás percepciones son las que configuran su precio, por lo que es natural la existencia de volatilidad en el precio de cualquier criptomoneda.

El precio en un momento determinado no es más que el monto al cual se transacciona entre oferentes y demandantes en ese momento.

Los casos de uso que una criptomoneda pueda tener, así como la escasez relativa de su oferta frente a la demanda que exista en el mercado hacen de ella un activo de mayor o menor valor para las personas.

Bitcoin, por ejemplo, basa su fortaleza en una oferta establecida de antemano: nunca habrá más de 21 millones de bitcoin en circulación, lo que lo hace sumamente escaso. Si agregamos a esa oferta restringida una demanda creciente por la variedad de casos de uso que le asignan las personas, obtenemos un precio en aumento.

VII. ¿Cómo se las puede adquirir?

A grandes rasgos, podemos decir que hay dos formas de adquirir criptomonedas. La primera consiste en comprarlas a través de un exchange o broker, por ejemplo, como Belo.app. Se trata de una plataforma que permite a las personas ingresar moneda local desde una cuenta bancaria o tarjeta de crédito, para comprar desde ella la criptomoneda deseada.

Los exchanges brindan la posibilidad a los usuarios de crear órdenes de compra y venta, por lo que únicamente intermedian las transacciones entre ellos, cobrando una comisión pequeña sobre los montos. Sin embargo, también es posible comprar directamente al bróker, lo que es recomendable para usuarios que dan sus primeros pasos en el mundo cripto. En este caso, la plataforma ofrece un precio de venta directamente al usuario, con una interfaz más simple.

La otra forma posible de comprar criptomonedas es la modalidad peer-to-peer. Consiste en realizar un intercambio de criptomonedas por fuera de cualquier plataforma, directamente entre dos partes: el vendedor envía el saldo en criptomonedas al comprador, que le transferirá el precio equivalente de la forma deseada, ya sea a través de un banco, en efectivo o en especies.

VIII. ¿Como funciona el registro contable compartido, o blockchain?

La cadena de bloques es una especie de base de datos, donde la información se almacena en los mencionados "bloques" de tal manera que se forma un registro inalterable. La

tecnología blockchain puede almacenar distintos tipos de datos: en el caso de Bitcoin, por ejemplo, se limita a registrar las transacciones que realicen los usuarios unos a otros, como si se tratara de un libro contable. En el caso de Ethereum, busca alojar aplicaciones descentralizadas

El registro es público: los datos que allí se almacenan están al alcance de todos. Cada nodo de la red guarda a su vez una copia completa de la cadena de bloques. Eso significa que blockchain no se aloja en un solo lugar, sino en cada integrante de la red. Así, la información está disponible en todo momento, sin riesgos de que pueda caerse o atacarse un servidor único.

Esta descentralización agrega una capa extra de seguridad : un atacante puede dirigirse a un nodo de la red, pero no podrá atacar a todos al mismo tiempo.

IX. ¿Qué implica que el registro sea de consenso?

Cada vez que se conforma un bloque con transacciones, los nodos que componen la red verifican su validez. Ellos son quienes deciden sobre la cadena de bloques correcta. La cadena válida es la que reúne el consenso de sus integrantes.

Alterar maliciosamente la cadena de bloques es computacionalmente muy complejo . Para que una modificación sea considerada válida por los nodos, más del 50% de ellos debería contener la información falsa. La cadena completa debería modificarse en cada uno de los nodos para que sea tomada como la cadena correcta. A mayor cantidad de nodos que integran la red, más difícil será para un atacante individual alterar el consenso logrado sobre la cadena de bloques.

X. ¿Por qué no puede alterarse un bloque?

La inalterabilidad de un bloque crece a medida que se suman nuevos bloques a la cadena: cada uno de ellos se vincula a través de tecnología criptográfica con el anterior. En caso de modificarse la información que almacena el bloque, su vinculación con el bloque previo se vería dañada, por lo que los nodos, encargados de verificar la validez del bloque, lo considerarían rápidamente inválido.

Así, se logra que el contenido de los bloques, y por ende de la cadena, sea inmutable, y se pueda asegurar su autenticidad, una característica que crece a medida que se extiende la cadena.

Blockchain nos permite almacenar información que no podrá modificarse, perderse ni borrarse . Así como Bitcoin fue la primera aplicación de este tipo de tecnología a una moneda digital, actualmente los casos de uso no paran de crecer. El concepto de una base de datos inmutable y descentralizada cuya integridad está garantizada por tecnología criptográfica es atractivo para certificar y validar cualquier tipo de información.

Ethereum ha avanzado desde su creación en esta dirección, con una blockchain programable, que cuenta hasta el momento con la mayor cantidad de aplicaciones descentralizadas (DApps) construidas en su red con distintos fines.

