

Historia y Evolución

Las criptomonedas surgieron del deseo de crear una forma de dinero digital segura, descentralizada y sin la necesidad de intermediarios. En esta sección se explora cómo nacieron las criptomonedas y cómo se han desarrollado desde su creación.

La historia de las criptomonedas no comienza con Bitcoin, sino con ideas y conceptos anteriores que sentaron las bases para lo que eventualmente se convertiría en la primera criptomoneda del mundo. Proyectos y propuestas como B-Money de Wei Dai y Bit Gold de Nick Szabo exploraron la idea de una moneda digital descentralizada, aunque ninguno llegó a materializarse en una red funcional. Estos conceptos, sin embargo, introdujeron ideas cruciales como la criptografía para asegurar transacciones y la descentralización para eliminar intermediarios.

La verdadera revolución comenzó el 31 de octubre de 2008, cuando una persona o grupo bajo el pseudónimo de Satoshi Nakamoto publicó el whitepaper de Bitcoin. Este documento presentó una solución al problema del doble gasto mediante el uso de una red de prueba de trabajo descentralizada. Bitcoin se lanzó en enero de 2009, marcando el nacimiento de la criptomoneda como la se conoce hoy. Con Bitcoin, Nakamoto no solo creó la primera moneda digital descentralizada sino también introdujo el concepto de blockchain, una cadena de bloques que registra todas las transacciones de manera segura y transparente.

A medida que Bitcoin aumentaba en popularidad y su valor comenzaba a ser reconocido, surgieron nuevas criptomonedas intentando mejorar aspectos de Bitcoin o proponer funcionalidades adicionales. Litecoin apareció como una "plata digital" en contraposición al "oro digital" que era Bitcoin, ofreciendo tiempos de confirmación más rápidos. Otras criptomonedas, como Ripple, buscaron facilitar las transacciones transfronterizas entre bancos de manera más eficiente.

En 2015 se produciría el lanzamiento de Ethereum, una criptomoneda que cambiaría la manera de ver las cosas. Creada por Vitalik Buterin y su equipo, Ethereum amplió el concepto de criptomoneda al introducir contratos inteligentes: programas que se ejecutan en la blockchain y permiten la creación de aplicaciones descentralizadas. Ethereum abrió la puerta a muchas posibilidades más allá de las transacciones financieras, sino también a juegos descentralizados, finanzas descentralizadas (DeFi) y más cosas que se discutirá en apartados posteriores.

Desde sus humildes comienzos con la publicación del whitepaper de Bitcoin, las criptomonedas han recorrido un largo camino, evolucionando de una simple moneda digital a una amplia gama de aplicaciones descentralizadas y sistemas financieros. Por último, cabe destacar la gran evolución que han tenido monedas como bitcoin en los últimos 10 años, de ser una simple moneda virtual sin valor a convertirse en una reserva de valor.

2. Monedas, Altcoins y Tokens

En la blockchain hay muchos tipos de criptomonedas que resuelven distintos problemas, se va a analizar cuales hay para posteriormente analizar una serie de proyectos que pueden ser interesantes.

En general se dice de una Altcoin a todas aquellas criptomonedas que no sean Bitcoin, ya puede ser Ethereum u otras como Ripple o Litecoin. Además, están las monedas, que son diferentes a las Altcoins ya que están basadas en su propia blockchain. Es decir, Bitcoin por ejemplo es la misma moneda que su blockchain así como Eth es la moneda de Ethereum.

Los Tokens representan ciertos activos o funciones en una blockchain. Todos estos son Altcoins pero se diferencian en que estos existen sobre una blockchain pero no son propios de la misma.

Estos tokens están incrustados en programas o códigos autoejecutables y pueden funcionar sin una plataforma de terceros. Facilitan smart contracts en la blockchain y también son fungibles y negociables. Los tokens también pueden usarse para representar puntos en un proyecto y bienes, a los que se le asocia un valor.

2. Monedas, Altcoins y Tokens

2.1. Tokens de Utilidad

Los tokens de utilidad o "utility tokens" son unidades que representan un valor en la blockchain y normalmente asociados a un producto o servicio que es ofrecido por el emisor del mismo.

Mientras seas titular, tendrás derecho al producto o servicio por el valor del token, pero no a la propiedad de este. Estos tokens son útiles porque facilitan el acceso a funciones o servicios en una plataforma digital basada en blockchain. Por ejemplo, podrían darte la capacidad de votar en decisiones importantes dentro de una comunidad digital, acceder a aplicaciones específicas o incluso usarlos como moneda dentro de un ecosistema digital para comprar servicios o productos exclusivos de esa plataforma.

Otro ejemplo; el acceso a almacenamiento descentralizado en una red de almacenamiento o tokens de recompensa podría ser una de las aplicaciones de tokens de utilidad.



Se muestra lo explicado anteriormente, como se te dará un access key para el servicio en la plataforma del blockchain.

Lo más importante es que los tokens de utilidad no son de inversión que puedan perder su valor a expensas del titular.

Por ejemplo, Filecoin es un token que se encarga del almacenamiento de datos de manera descentralizada.

2. Monedas, Altcoins y Tokens

2.2. Tokens de Seguridad

Los tokens de seguridad ("security tokens") son monedas que representan un interés en activos externos. Estos activos pueden incluir propiedades, bonos, acciones, bienes y otros. Son útiles por ejemplo cuando los inversores necesitan liquidación inmediata o transparencia en la gestión, y se pueden negociar como valores.

Estos tokens se ofrecen a través de Ofertas de Tokens de Seguridad (STO), que están reguladas por entidades financieras. Esta regulación busca proteger a los inversores, asegurando la transparencia y la equidad en la inversión. La naturaleza fraccionada de los tokens de seguridad permite inversiones más accesibles en activos costosos, abriendo nuevas oportunidades para inversores no tradicionales.

Gracias a la tecnología blockchain, la propiedad y la transferencia de estos tokens se realizan de manera segura y eficiente, promoviendo una inversión más directa y menos dependiente de intermediarios.

2. Monedas, Altcoins y Tokens

2.3. Tokens de Pago

Los tokens de pago son criptomonedas diseñadas para intercambiar o para comprar bienes o servicios. Actúan de manera similar al dinero tradicional dentro de sus respectivos ecosistemas digitales o en plataformas que los aceptan. A diferencia de los tokens de seguridad, que representan una inversión y están sujetos a regulaciones financieras, los tokens de pago facilitan transacciones rápidas, seguras y con costos de transacción más bajos que los sistemas convencionales.

Bitcoin, considerado por muchos como la primera criptomoneda, es el ejemplo más conocido de un token de pago, aunque su valor y uso como reserva de valor a veces lo sitúan en una categoría propia.

2. Monedas, Altcoins y Tokens

2.4. Tokens de Intercambio

Los tokens de intercambio desempeñan un papel crucial en las plataformas de comercio de criptomonedas, facilitando la compra, venta e intercambio de criptomonedas.

Estos tokens pueden ser lanzados tanto por exchanges centralizados como por plataformas descentralizadas, y su función principal es simplificar las transacciones entre tokens o servir como medio de pago de servicios en dichas plataformas. El uso de tokens de intercambio ofrece varios beneficios, incluyendo la reducción de costes (gas fees), mejora de liquidez, descuentos de las plataformas por usarlos u otros privilegios dentro de los exchanges.

Binance Coin, podría ser una moneda de este tipo en el exchange centralizado Binance.

2. Monedas, Altcoins y Tokens

2.5. NFT (Non Fungible Token)



Las NFTs, o Tokens No Fungibles, son versiones digitales únicas de obras de arte, coleccionables o cualquier otro ítem virtual, respaldadas por blockchain, que certifican su autenticidad y propiedad. A diferencia de las criptomonedas tradicionales, intercambiables y uniformes, cada NFT es irrepetible, otorgando un valor especial basado en su singularidad y demanda.

Este concepto ha revolucionado el arte digital y el coleccionismo, permitiendo a los creadores obtener ingresos directos mediante ventas y regalías continuas. Además, las NFTs se extienden a otros ámbitos como los videojuegos y coleccionables digitales, y exploran aplicaciones en propiedades y bienes físicos. A pesar de sus beneficios, las NFTs enfrentan debates sobre su impacto ambiental y cuestiones legales de derechos de autor, marcando un territorio emergente en la economía digital.

Ejemplos de colecciones de NFTs famosas y con renombre podría ser Bored Ape Yach Club. Una de sus colecciones de arte digital se ve así:

2. Monedas, Altcoins y Tokens

2.6. DeFi Tokens

Finanzas Descentralizadas, o DeFi, representa un conjunto de aplicaciones financieras construidas sobre plataformas de blockchain que funcionan de manera descentralizada, abriendo el acceso a servicios financieros a cualquier persona con acceso a internet. A través de DeFi, los usuarios pueden ganar intereses, ahorrar, gestionar fondos, invertir, comprar y vender activos, realizar transacciones y participar en mercados descentralizados sin la necesidad de intermediarios tradicionales.



Los tokens DeFi son el corazón de este ecosistema, actuando como dinero programable que impulsa estas aplicaciones. Estos tokens no solo facilitan las transacciones dentro de las plataformas DeFi, sino que también permiten la creación y el comercio de activos digitales en un entorno seguro y transparente. La mayoría de estas soluciones se han desarrollado en la blockchain de Ethereum, aprovechando su robusta infraestructura para contratos inteligentes. Sin embargo, otras blockchains como Stellar, Polygon, Tron y Cardano también están emergiendo como plataformas compatibles con aplicaciones DeFi, ampliando el espectro de posibilidades.

Ejemplos de DeFi podrían ser UniSwap o PancakeSwap que son DeFi exchanges con su propio token.

2. Monedas, Altcoins y Tokens

2.7. Stable Coins

Las criptomonedas llamadas stablecoins tienen el propósito de mantener un valor estable en relación con un activo específico, generalmente una moneda fiduciaria como el dólar estadounidense. La estabilidad de las monedas tradicionales y la flexibilidad y seguridad de

la tecnología blockchain se combinan en este diseño. Por lo tanto, las criptomonedas estables solucionan uno de los mayores problemas con los que se enfrentan las criptomonedas tradicionales: la volatilidad del precio.

La estabilidad de estas monedas se logra de varias maneras, cada una de las cuales depende del diseño particular de la moneda estable. Algunas están respaldadas directamente por las reservas de la moneda a la que están atadas; por cada stablecoin en circulación, hay una cantidad equivalente al activo de reserva guardado por el emisor de la stablecoin.

Algunos utilizan métodos automatizados para ajustar la oferta de la moneda en circulación y mantener el precio estable, utilizando algoritmos complejos.

Dentro del ecosistema de las finanzas descentralizadas (DeFi) y más allá, estas monedas tienen una amplia gama de usos prácticos. Permiten a los usuarios ahorrar, prestar o realizar transacciones con la confianza de que su valor no estará sujeto a la volatilidad que caracteriza a otras criptomonedas. Esto las hace especialmente útiles para el comercio internacional y las remesas, así como como refugio seguro para los comerciantes e inversores del mercado de criptomonedas.

Entre las stablecoins más conocidas se encuentran Tether (USDT), USD Coin (USDC) y DAI. Tether y USD Coin están respaldados por dólares estadounidenses u otros activos equivalentes, mientras que DAI utiliza un sistema de garantías en criptomonedas y mecanismos automatizados para mantener su paridad con el dólar.

2. Monedas, Altcoins y Tokens

2.8. Tokens Respalados por Activos y RWA (Real World Assets)

Los tokens respaldados por activos se definen como criptomonedas cuya valoración se sustenta directamente en activos tangibles o intangibles. De esta manera, pueden simbolizar una parte proporcional de bienes físicos como un lingote de oro, propiedades inmobiliarias, obras de arte o incluso activos intangibles como patentes de invención. Este tipo de tokens transforma la adquisición, transferencia y comercialización de dichos activos, haciéndolos más accesibles, modernos y eficientes mediante el uso de la tecnología blockchain, asegurando así una legítima propiedad.

Uno de los principales atractivos de los tokens respaldados por activos es la fusión entre los beneficios de la tecnología blockchain y la estabilidad inherente al activo subyacente. Esta sinergia resulta en inversiones menos complejas, incrementa la liquidez de los activos representados y fomenta la confianza en el valor del token, dado que este último se ancla a un bien de valor real y verificable.

Los tokens respaldados por activos representan una fracción del activo total, pudiendo sus poseedores poseer el derecho íntegro al reclamo o recibir de alguna forma proporcional al token, dicho derecho. Su emisión y verificación suelen estar realizados a través de plataformas que garantizan su correspondencia con el valor total del activo, mediante auditorías y controles periódicos. De esta forma, el token se encuentra enlazado al valor y posesión del activo total, constituyendo así una moneda electrónica real y no ficticia.

¿Qué son los RWA?

Los "Real World Assets" (RWA), traducidos al español como "Activos del Mundo Real", son activos tangibles que existen fuera del ámbito digital o virtual. Estos activos representan bienes físicos con valor económico, como propiedades inmobiliarias, terrenos, maquinaria, equipos, obras de arte, productos naturales (como metales preciosos o productos agrícolas), entre otros.

Los RWA son elementos con valor intrínseco que pueden generar ingresos, apreciarse con el tiempo o proporcionar utilidad de alguna manera. A diferencia de los activos financieros, como acciones o bonos, los RWA tienen una presencia física y su valor se deriva de su utilidad, demanda en el mercado, escasez y otros factores relacionados con sus características físicas.

En el contexto de la tokenización de activos, los RWA se pueden representar digitalmente mediante tokens en una blockchain. Esta tokenización permite fraccionar la propiedad de los activos, lo que significa que los inversionistas pueden poseer una parte de un activo físico a través de la tenencia de tokens. Por ejemplo, una propiedad inmobiliaria se puede tokenizar, lo que permite a múltiples inversionistas poseer partes de la propiedad y participar en sus ingresos potenciales, como alquileres o ganancias por su venta.

La tokenización de RWA tiene varias ventajas, incluida la mayor liquidez de los activos, la facilidad de transferencia de propiedad, la reducción de barreras de entrada para los inversionistas y la creación de nuevos mercados financieros más eficientes y accesibles. Además, la transparencia y la seguridad inherentes a la tecnología blockchain pueden mejorar la confianza en los mercados de activos del mundo real y facilitar la inversión global.

2. Monedas, Altcoins y Tokens

2.9. Tokens de Privacidad

Las criptomonedas de privacidad se utilizan para aplicaciones relacionadas con la privacidad, como su nombre indica. Es diseñado para brindar mayor anonimato y privacidad durante las transacciones y otras actividades.

Las transacciones criptográficas requieren una mayor privacidad por varios motivos. El primero es un derecho fundamental, pero también es necesario para investigaciones de seguridad y transacciones muy delicadas. Sin embargo, las criptomonedas de privacidad se utilizan con cierta frecuencia en actividades delictivas o fraudulentas.

Las criptomonedas de privacidad protegen las transacciones mediante la combinación de monedas y transacciones sin conexión. Además, utilizan métodos similares a los de otras criptomonedas, como no vincular nombres reales a direcciones criptográficas y cifrar la cadena de bloques.

Ejemplos de tokens de privacidad pueden ser Monero o ZCash.