



GLOSARIO CRYPTO

A

Airdrop: Cuando se le regala una cantidad de tokens o criptomonedas a una comunidad interesada. Muchas veces se utiliza como estrategia para captar la atención de dicha comunidad.

Allocation: Es una asignación de tokens o capital, que se puede ganar, comprar o reservar para un determinado inversor, equipo, grupo, organización u otra entidad relacionada.

AMA (Ask me Anything): Es una sesión abierta donde los interesados pueden preguntar de todo en relación a un proyecto.

AML (Anti-money Laundering): Agrupación del conjunto de leyes, normativas y procedimientos o métodos que se utilizan para aclarar la procedencia del dinero de un inversor, se enfocan en evitar que los delincuentes oculten el origen ilegal de su dinero.

AMM (Automated Market Maker): Creador automático de mercado, es un protocolo programado que sigue una serie de fórmulas matemáticas y económicas con el fin de crear un medio equilibrado que permitan a los usuarios de dicho protocolo llevar a cabo intercambios de criptomonedas de forma segura. Ejemplo: Uniswap.

Apalancamiento - Leverage: El apalancamiento financiero consiste, básicamente, en endeudarse para invertir. Su funcionamiento se basa en recurrir a la deuda, que permite al usuario invertir más capital del que tiene gracias al que ha pedido prestado.

Asset: Activo. Cualquier bien (ya sea del mundo digital o del mundo físico) con capacidad para ser tokenizado, y que tenga interés o valor para los demás.

Atomic Loans: Empresa centrada en la creación de préstamos en stablecoins respaldados por Bitcoin sin custodia.



GLOSARIO CRYPTO

B

BackEnd: Es la acción de mover activos desde una blockchain a otra a través de un servicio centralizado llamado "bridge". Los tokens que no son nativos de una blockchain pero existen en otras se denominan wrapped tokens.

Barbell: Se trata de dividir la cartera de inversión en dos partes: Una, con un riesgo muy reducido, sin volatilidad, y la otra, con un nivel de riesgo elevado, aunque siempre dentro de cierta ponderación, sin arriesgar en exceso.

Blockchain: Registro único y descentralizado donde, donde la información se almacena en bloques separados que están criptográficamente relacionados por medio de un "Hash" (la definición de Hash está más abajo , en la H).

Bonding Curve: Curva matemática que establece una relación directa entre el precio de un token y su oferta (supply), actuando como un Automated Market Maker (AMM). De esta manera, el precio del token aumenta automáticamente cuando hay una compra, y disminuye al haber una venta, y los tokens son destruidos.

Bot: Programa informático que efectúa automáticamente tareas repetitivas. Puede estar diseñado en cualquier lenguaje de programación.

Bóveda: Antiguamente conocida como CDP (Posición de Deuda Colateralizada), es un smart contract donde depositas un colateral y tienes a cambio derecho a generar un préstamo contra dicho colateral.

Bridge: Permite intercambiar información bidireccional entre blockchains mediante un protocolo que permite la conexión.



GLOSARIO CRYPTO

C

Cap Table: Se trata de una tabla que muestra quiénes son los dueños del capital social de una compañía, quiénes son sus socios con sus respectivos porcentajes. Suele incluir el porcentaje de cada socio, el total de participaciones de una sociedad, el número de participaciones de cada socio y la valoración de las diferentes rondas de inversión.

CBDC (Central Bank Digital Currency): Las monedas digitales de los bancos centrales son tokens digitales, emitidas por un banco central. Están vinculadas al valor de la moneda fiduciaria de ese país.

CeFi (Centralized Finance): Hace referencia al mercado de finanzas donde las operaciones están custodiadas por un tercero (normalmente una empresa), en oposición a DeFi (Decentralized Finance).

Clave Privada: Clave que permite la total propiedad y manejo de un wallet (monedero de criptomonedas).

Clave Pública: Identificador de una cuenta de Blockchain. Es como el número de una cuenta bancaria o el nombre de usuario de cualquier cuenta de una página web. Cualquier persona puede tener esta información, pero para acceder necesita la clave privada.

Cliff: El período de congelación de tokens asignados a una wallet.

Colateral: El colateral es un activo que sirve como garantía frente a la concesión de un crédito, una emisión de bonos o cualquier otra operación financiera. Un ejemplo de sobrecolateralización con criptomoneda es la stablecoin DAI emitida por MakerDAO. Los usuarios pueden sobrecolateralizar activos digitales (ETH, BTC, etc.) a través de contratos inteligentes "Collateralized Debt Positions" (CDP) y luego acuñan la cantidad correspondiente de DAI como su deuda sobrecolateralizada. El CDP bloqueará este activo hasta que los usuarios devuelvan la deuda DAI.



GLOSARIO CRYPTO

Colateralizar. Aportar una cantidad de criptomonedas como fondo de reserva para pedir un préstamo.

Criptomonedas: A contrario de las monedas que son emitidas por gobiernos y bancos centrales, las criptomonedas se crean al resolver problemas matemáticos que usan criptografía. Aun así, su valor puede variar debido a la oferta y demanda en los mercados.

D

DAO (Decentralized Autonomous Organization): Organización Autónoma Descentralizada. Se trata de una nueva forma de asociar los intereses de los participantes en un proyecto, cambiando la gobernanza centralizada habitual (en una empresa, CEO o similar) a un conjunto de smart contracts gobernados por los token holders.

DeFi (Finanzas Descentralizadas): Conjunto de aplicaciones y protocolos que permiten generar productos y servicios financieros sin la necesidad de un intermediario o agente mediador.

Deployar. Literalmente significa “despliegue” pero es un término utilizado en programación que, dependiendo de cada situación, podrá significar implantar, colocar en posición, habilitar para uso o, simplemente, publicar.

Derivados: Producto financiero cuyo valor depende de otro activo. En DeFi existe la versión tokenizada de los derivados a través de los assets sintéticos.

Desarrolladores: Profesionales dedicados a implementar software de aplicaciones o de sistemas. Cualquier aplicación que utilizamos ha sido programada por desarrolladores.

DEX (Decentralized Exchange): Mercado de criptodivisas descentralizado que funciona como una aplicación descentralizada que se ejecuta en una blockchain específica a través de smart contracts. Ejemplo: SushiSwap, ApeSwap, TraderJoe, Uniswap V3, Curve, Velodrome, etc.



GLOSARIO CRYPTO

Dificultad de minado: Dato utilizado para aumentar o disminuir la complejidad de la minería de bloques. Si la dificultad es alta, se necesita más poder de cómputo para extraer la misma cantidad de bloques y la red es más segura.

DPOS (Delegated Proof of Stake): Prueba de Participación Delegada. Protocolo de consenso diseñado para blockchains altamente escalables. Los participantes de la red eligen por votación "delegados" que permiten implementar el protocolo. No se utilizan equipos para minar de alta computación y gasto energético. La participación en la red para confirmar bloques depende de la cantidad de tokens que tiene cada usuario.

Dump: Vender a un precio inferior al de mercado.

Dusting Attack: Ataque por parte de un scammer que consiste en enviar tokens a una billetera con la premisa de que el holder de estos tokens interactúe con un Smart Contract para robar los fondos. Nadie regala dinero. Puedes ver estos tokens "raros" escaneando la dirección pública de tu wallet en una explorador de bloques.

E

Earn out: Derecho económico sobre la venta final de una compañía.

Ecosistema: Sistema que está formado por un conjunto de elementos, el medio en el que se desarrollan (hábitat) y las relaciones que se establecen entre ellos.

ERC20: Estándar de Ethereum que rige la creación de un smart contract con una tipología concreta de tokens, estandarizando la interfaz de creación y emisión de nuevos tokens en dicha red. Garantiza la interoperabilidad entre tokens.

Etherscan: Motor de búsqueda de la blockchain de Ethereum. Su objetivo es hacer que la cadena de bloques de Ethereum sea transparente, mostrando información clara e inequívoca sobre sus actividades. Permite ver todas las transacciones realizadas dentro de la red.



GLOSARIO CRYPTO

EVM (Ethereum Virtual Machine): Máquina virtual que forma parte del ecosistema blockchain de Ethereum. Puede ejecutar variedad de instrucciones, por lo que tiene una gran flexibilidad para realizar diferentes operaciones basadas en el lenguaje Solidity.

Exchange: Empresa necesaria para cambiar FIAT a Criptomonedas, y al revés.

F

Fake: Algo que de primeras parece cierto/verdadero/confiable pero que analizado desde ojos expertos resulta ser falso.

Farming: Aportación de liquidez a un protocolo y a cambio generación de tokens como recompensa (rewards) en un marco de tiempo limitado.

Fee: Coste de la ejecución de una transacción en la red: Satoshis para Bitcoin (BTC), Gwei para Ethereum (ETH).

FIAT: Dinero que existe "por decreto", impreso por alguna entidad central con competencias para ello (Dólares, Euros...).

Flash Loan: Préstamo sin colateral a través de un smart contract con varias partes estructuradas. Por un lado, se solicita un préstamo, se hacen las operaciones deseadas con él y, finalmente, se devuelve dicho préstamo en la misma transacción (en el mismo bloque de Ethereum).

Flipping de NFTs: Compraventa de NFTs, especular con NFT's (especular no es mala palabra).

FOMO (Fear of Missing Out): Sensación de ansiedad que lleva a comprar o vender de manera no tan razonada por temor a perderse "algo".

FrontEnd: Es lo que vemos y lo que interactuamos de un sitio web. Estilos, colores, fondos, interacciones, etc.

FUD: Diseminar información negativa.



GLOSARIO CRYPTO

Fully Dilluted Value o FDV: Proyección futura de la oferta circulante de un token en base a las emisiones e inflación previstas para el mismo.

Fungibilidad: “Que es intercambiable”. Un bien fungible es aquel bien que es reemplazable por otro de las mismas características. ejemplo: un Euro es Fungible porque es igual y tiene las mismas características que otro Euro.

G

Gas: Comisión pagada a los mineros/validadores para que funcione el ecosistema. En Bitcoin le llamamos fees.

Gwei: 10^9 wei es un gwei. Gwei es la unidad más común cuando se habla de gas (costes de transacción). En vez de decir que el coste de gas de una operación es 0.000000001 ETH se puede decir 1 Gwei.

H

Hard-fork: Es una actualización importante del protocolo que obliga a todos los usuarios a pasar al nuevo software si quieren seguir usando la misma cadena de bloques. Este proceso genera una bifurcación de la red, por lo que hay que elegir si queremos seguir usando la nueva versión o la antigua.

Hash: resultado de una función matemática que convierte cualquier bloque de información en un código alfanumérico de longitud fija, es el equivalente informático de la huella digital de un bloque de información. Habitualmente trabajamos en Blockchain con la versión SHA-256.

Health factor. Parámetro que mide la calidad (riesgo) de una posición de deuda en un protocolo DeFi. Un health factor bajo provocará que la posición se liquide.

Hodl o Holdear. Mantener en cartera los token o criptomonedas sin hacer ninguna operación con ellos. Su precio variará en función de las variaciones que sufra el mercado.



GLOSARIO CRYPTO

I

IC (Identidad Corporativa): Son los aspectos visuales (diseños, colores, formas, tipografías, etc) que forman la identidad de una marca o una empresa.

Impermanent Loss: Cuando hablamos de impermanent loss o pérdida no permanente, hacemos referencia a un proceso que se da cuando aportas una cantidad de liquidez en un Liquidity Pool. Se produce cuando el precio de tus tokens cambia respecto al momento en que los depositaste. Cuanto mayor sea este cambio, más grande será la pérdida. Este indicador mide el costo de oportunidad al optar por estrategias de "Liquidity Provider" o LP.

Invariante de un pool: Fórmula que permite calcular los precios de los tokens de un pool, en función de su oferta y demanda. La siguiente fórmula permite el cálculo. $\text{Invariant} = \text{N}^\circ \text{ de tokens "A"} \times \text{N}^\circ \text{ de Tokens "B"}$. El invariant se ha de mantener constante en el pool, de manera que el aumento o disminución de precio de uno de los tokens, hace que el otro token realice la operación contraria para que el "Invariant" se mantenga estable.

K

KYC (Know your customer): Documento por el cual se identifica al usuario de una wallet y lo une a un DNI/CIF. Resulta necesario en la emisión de security tokens.

L

Lending: Prestar o depositar tokens en un pool y recibir interés por prestar esta liquidez.

Liquidity mining: Estrategia a través de la cual un inversor añade liquidez a un protocolo a cambio de token nativos del mismo.

LP Liquidity Provider. Aquella persona que proporciona liquidez a un pool, a fin de recibir "fees" por cada uno de los intercambios que se realicen en él (swaps).



GLOSARIO CRYPTO

LP token: Es un token creado de dos criptomonedas, se utiliza para hacer farming y recompensa a los proveedores de liquidez en los intercambios descentralizados.

M

Market Cap: Es el valor de las acciones en circulación de una empresa. En el mundo crypto es el valor en dólares de los tokens en circulación de una criptomoneda.

Mineros: Hardware especializado en la resolución de algoritmos sobre los que se basa y se mantiene segura una blockchain.

Mintear: Es en un término más literal significa «acuñar», crear un objeto digital único dentro de una blockchain. Como quien acuña una moneda.

MOFO: Término empleado cuando sucede lo contrario al FOMO y existe ansiedad por realizar ventas no razonadas por temor a desplomes.

N

Nodos: Red de Computadoras interconectadas que comparten información de forma segura y descentralizada en una blockchain. Todos los nodos tienen el mismo peso y operan de la misma manera. Los nodos ejecutan un software determinado, como es el caso de Bitcoin y se sincronizan entre ellos. Todos los nodos siguen las mismas reglas, aunque pueden desarrollar distintas funciones.

Nonce: "Número de un solo uso", utilizado en los algoritmos de Prueba de Trabajo (PoW) para determinar el minero que se lleva la recompensa de cada bloque minado. El nonce se determina por esfuerzo computacional y forma parte de la información crítica de cada bloque minado al estar incorporado en la cabecera de cada bloque.



GLOSARIO CRYPTO

O

Oferta circulante (circulating supply): Cantidad total de tokens que están en el mercado.

Off Chain: Los datos off chain son transacciones fuera de la blockchain. Esto permite tener menores costos de transacción y mayor velocidad. Ejemplos: Lightning Network, Roll ups, ZK Rollups, Sidechain, P2P en Exchanges.

OG (Original gangster): Término que proviene de la cultura hip-hop. Significa que la gente que estuvo aquí desde el principio, se ganó un respeto.

On Chain: Los datos on chain son transacciones realizadas en una blockchain pública a los cuales todos tenemos acceso.

Open source: Código abierto. Cualquier persona o entidad tiene capacidad para acceder al código de un protocolo, programa, contrato, etc., y modificarlo para adaptarlo a sus necesidades.

Oráculo: Conexión existente entre un smart contract y el mundo real para obtener información necesaria para la ejecución del mismo (precios, horarios, etc).

P

Pegged: Un activo digital cuyo valor está vinculado al de algún otro medio de intercambio, como el oro o la moneda de una nación determinada.

Pool de liquidez: Aportación de liquidez a un protocolo de cambio entre dos o más tokens y a cambio recibir una parte proporcional de las fees que se generan en dicho pool.

Pool DeFi: Nueva versión del concepto clásico de Exchange pero descentralizado, donde en vez de fijar los precios de los activos por libros de órdenes utilizamos algoritmos; en función del tipo y cantidad de tokens inyectados al pool obtenemos precios por los assets. Cualquier pool necesita de LPs.



GLOSARIO CRYPTO

Proof of Adress: Prueba de domicilio. En wallets se aplica a la prueba de residencia del país del titular de cuentas de Exchange o wallets custodiados. Habitual en un proceso de KYC y AML.

Proof of importance (POI): Sistema que se utiliza para determinar qué usuarios son elegibles para realizar los cálculos necesarios para agregar un nuevo bloque de datos a una cadena de bloques y recibir el pago asociado. Prioriza a los mineros en función tanto del staking como del número de transacciones en la criptomoneda correspondiente que realizan. Cuantas más transacciones se realicen hacia y desde la billetera de criptomonedas de una entidad, mayores serán las posibilidades de que la entidad reciba proyectos mineros.

Proof of Stake (POS): Protocolo de consenso para redes distribuidas que protege el sistema al solicitar prueba de posesión de la moneda. Con PoS la probabilidad de encontrar una transacción y recibir el bono correspondiente es proporcional a la cantidad de monedas acumuladas (evitando así que la confianza se determine por la cantidad de trabajo invertido).

Proof of work (POW): Protocolo de consenso que mide el esfuerzo computacional que aporta cada minero a la red para recompensar al que encuentre la prueba matemática que le permita recibir la recompensa por minar el bloque. El POW defiende la red frente a ataques a través del "hashrate".

Protocolo: Son las reglas que forman un lenguaje codificado con una sintaxis, semántica y procedimientos definidos, para que se entiendan, comuniquen y sincronicen dispositivos conectados a una red.

Pump: Hinchar el precio de un activo (para que suba).

R

Ratio de Sharpe: Una relación creada en 1966 y que los inversores y economistas utilizan para evaluar el retorno potencial de la inversión (ROI).



GLOSARIO CRYPTO

Ratio de Treynor: Mide el exceso de rentabilidad ganado por unidad de riesgo sistemático.

Rekt: Que ha perdido todo lo invertido por un movimiento brusco del mercado.

Riesgo sistémico: Riesgo del mercado independiente del activo en cuestión. Es decir, riesgo no diversificable entre activos del mismo conjunto.

ROI (Return on Investment): retorno de la inversión.

S

SAFT (Simple Agreement for future Tokens): Documento que se usa, habitualmente, en los inicios de un proyecto donde una empresa emite tokens y los inversores adquieren el derecho de los mismos.

Security Token: Es un tipo de token criptográfico vinculado a valores financieros. Otorgan a los propietarios derechos y obligaciones. Está respaldado por un bien del mundo tangible o intangible.

SHA-256: Función hash que ha sido elegida para el funcionamiento de muchas criptomonedas (Bitcoin entre ellas). Ofrece un alto nivel de seguridad, protege y codifica de forma segura la información de las mismas. Garantiza la integridad de la información almacenada en un bloque, entre otras cosas. Desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y el National Institute of Standards and Technology (NIST).

Shorting: Estrategia de vender un token cuyo precio se estima a la baja por una stablecoin y volver a comprarlo antes de que vuelva a recuperar.

Sidechains: Una cadena lateral es una cadena de bloques basada en una blockchain matriz principal. El uso de cadenas laterales permite la creación de varios tipos de contratos inteligentes, acciones, derivados, etc. Mejora las prestaciones de una blockchain ya existente al permitir funcionalidades no viables en la nativa.



GLOSARIO CRYPTO

Sintéticos: Activos que copian el movimiento de precio de otro pero sin estar vinculados, permitiendo la exposición a dicho activo y cubriendo el riesgo con distintos tipos de colateral.

Skin in the game: Dejarse la piel en el Juego como traducción literal, sería tomar verdadero riesgo al implicarse realmente en lo que haces.

Slippage: Valor en % de cambio permitido del valor de los tokens durante un proceso de swapping (intercambio).

Snapshot: Es registrar el estado de una blockchain en un momento dado.

Soft-fork: Es una actualización del código del programa que gestiona una blockchain para añadir un cambio, normalmente una funcionalidad nueva o corrección de algún error. Pero para ser un soft-fork debe seguir siendo compatible con la blockchain antigua.

Stablecoin: Cripto ligada a un activo financiero real (oro, dólar,...). Token de valor estable colateralizado con assets del propio ecosistema blockchain o del sistema tradicional.

Stake: Mantener fondos bloqueados en bóvedas, smart contracts o protocolos, como depósito, para recibir recompensas.

Stress de un pool: Nivel de liquidez disponible respecto a los activos depositados. Se dice que un pool está estresado cuando tiene poca liquidez al haber realizado operaciones en las que se ha producido una gran descompensación de tokens, por lo que el precio que devuelve el pool por cada token es malo en términos de eficiencia.

Swap: Swap se refiere a intercambiar un criptoactivo por otro, esto conlleva a un gasto de gas, como cambiar tu BTC por ETH, pero siempre utilizando la misma blockchain.



GLOSARIO CRYPTO

T

TGE (token generation event): Momento donde se genera el token en una blockchain y su lanzamiento al mercado en cualquiera de sus formas de venta (privada, pública o ICO).

Token: Representación digital de un asset con unas características determinadas según la funcionalidad del mismo.

Token de Gobernanza: La gobernanza son las reglas que permiten el desarrollo y mantenimiento de una red o de un protocolo. El poseedor de tokens de gobernanza participa en las votaciones que propone la comunidad y así se toman las decisiones. La gobernanza puede ser descentralizada totalmente, parcialmente o centralizada.

Token holder: Poseedor de un token.

Tokenización de activos: Representación digital de todo aquello que tenga un valor que alguien esté dispuesto a pagarlo.

Tokenomics: Reglas que rigen el funcionamiento de un token entre todos sus participantes (cantidad, proporción del total, características, etc).

TPS (transacciones por segundo): Cantidad de transacciones por segundo que es capaz de procesar una red blockchain.

TVL (Total Value Locked): La cantidad de fondos que están bloqueados como garantía en un protocolo DeFi por el precio actual de los activos.

Txn: Transacción.



GLOSARIO CRYPTO

U

Unlock: Cuando un token se desbloquea.

Utility Token: Token cuya utilidad reside en tener un derecho de acceso a productos o servicios sobre futuros desarrollos del proyectos. Suelen estar destinados a financiar un proyecto, aunque también se pueden emitir en un contexto de no buscar financiación.

UTXO: Salida de transacción no gastada o Unspent Transaction Output. Salida de transacción no gastada o Unspent Transaction Output.

V

Vampire mining: Cuando un hard fork consigue llevarse todo el negocio del proyecto forkeado. El nuevo proyecto le da mejores condiciones a la comunidad con el objetivo de que trasladen los fondos del proyecto original al nuevo.

Vesting: Es un periodo de bloqueo de tokens con una duración específica y unas condiciones de desbloqueo.

VFA (Virtual financial Asset): La ley define un activo financiero virtual como cualquier forma de registro en un medio digital que se utiliza como medio digital de intercambio, unidad de cuenta o depósito de valor y que no es dinero electrónico, un instrumento financiero o un token virtual.

Volatilidad: Mide la rapidez de la variabilidad o fluctuaciones del precio de un activo y su rentabilidad. Volatilidad Histórica: Se expresa en porcentaje y se calcula como la desviación que registra un activo con respecto a su media de cotización histórica en un periodo determinado.

W

Wallet: Programa o accesorio que almacena tus criptodivisas.

Whitelisteado: Es el proceso por el cual se registran las wallet de los participantes en el proyecto.



GLOSARIO CRYPTO

Whitepaper. Documento que explica con detalle un proyecto de lanzamiento de un token o protocolo. En él se detalla el proyecto, financiación, tokenomics, problemas que resuelve y la hoja de ruta de su puesta en marcha.

Wrappear. Crear una versión 2 sobre un token que ya existe, ya sea en otra cadena o en otro protocolo. La denominación de este nuevo token tiene el nombre del original y alguna sigla delante que lo identifica. Por ejemplo wBTC es un wrapped token de BTC que corre en la cadena de Ethereum.

Y

Yield Farming: Actividades realizadas por los titulares de activos de criptomonedas en el uso de criptomonedas para invertir y obtener el mayor retorno de la inversión.