Glosario de términos técnicos utilizados en este libro

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Las entradas siguientes definen, por orden alfabético (según el término inglés), los términos técnicos utilizados a lo largo del libro en el sentido en que el libro los emplea. Cuando un término tiene una definición legal en el Derecho suizo o singapurense, la entrada lo indica y cita la fuente. Cuando tecnólogos y juristas usan un término de manera distinta, la entrada recoge el uso jurídico adoptado aquí. Las remisiones a otras entradas figuran en cursiva.

Account model (modelo de cuentas) — Diseño de registro en el que cada dirección tiene un saldo que aumenta y disminuye con las transacciones, como en Ethereum, a diferencia del *modelo UTXO* que utiliza Bitcoin. La distinción influye en cómo los tribunales rastrean los fondos y en cómo los custodios atribuyen los activos agrupados de los clientes.

Address (dirección) — Cadena de caracteres derivada de una *clave pública* que identifica un destino para tokens en un registro; cualquiera puede crearla sin coste y no lleva nombre alguno. Una dirección pasa a ser un dato personal conforme a la normativa suiza y singapurense de protección de datos en cuanto puede vincularse a una persona física.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Airdrop — Distribución gratuita de tokens a direcciones existentes, normalmente para recompensar a los primeros usuarios o para dispersar más la tenencia. Los airdrops tienen consecuencias fiscales como rendimiento o como adquisición a coste cero, según que el receptor tenga la condición de operador profesional (trader) o de inversor privado.

Algorithmic stablecoin (stablecoin algorítmica) — Token que intenta mantener un valor estable mediante ajustes de la oferta sin respaldo íntegro de garantías, cuyo ejemplo principal fue UST de Terraform hasta su colapso en mayo de 2022. Ni la FINMA ni la Monetary Authority of Singapore (MAS, la autoridad monetaria y supervisora financiera) tratan estos tokens como stablecoins a efectos regulatorios.

AMLA — Ley suiza contra el blanqueo de capitales (Geldwäschereigesetz, GwG/LBA), SR 955.0, que se aplica a los *intermediarios financieros* y que la FINMA interpreta en el sentido de que abarca a la mayoría de los proveedores que tienen poder de disposición sobre los criptoactivos de sus clientes.[1]

Asset-referenced token (ART, token referenciado a activos) — Categoría de MiCA, conforme al art. 3, apdo. 1, punto 6, del Reglamento (UE) 2023/1114, para un criptoactivo que mantiene un valor estable referenciándose a cualquier valor o derecho, o a una combinación de ellos, incluidas varias monedas. Es la contrapartida del *token de dinero electrónico* referenciado a una sola moneda.

Asset token (token de inversión) — Categoría de la FINMA para un token que representa un crédito o una participación en el capital, una participación en beneficios futuros o un derecho sobre un activo, conforme a la sección 3.1 de las Directrices sobre ICO de 16 de febrero de 2018. En casi todos los casos, estos tokens son valores mobiliarios según el Derecho suizo y conllevan consecuencias en materia de folleto y de licencias.

Automated market maker (AMM, creador de mercado automatizado) — Plataforma de intercambio descentralizada, cuyo ejemplo principal es Uniswap, que fija el precio de las operaciones mediante una fórmula frente a una liquidez

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

agrupada, en lugar de casar órdenes de compra y de venta. Según el análisis del capítulo VI, la contraparte de una operación en un AMM son los *proveedores de liquidez* del pool considerados en su conjunto.

Block (bloque) — Lote de transacciones que se añade a un registro como unidad y que contiene el *hash* del bloque anterior, de modo que los bloques forman una cadena cuya alteración cualquiera puede detectar.

Block explorer (explorador de bloques) — Sitio web, como Etherscan o mempool.space, que muestra de forma legible el contenido de un registro público. Un abogado debería ser capaz de leer una transacción en un explorador de bloques antes de emitir cualquier dictamen sobre ella.

Bridge (puente) — Mecanismo para representar en un registro un token de otro, normalmente bloqueando el original en un contrato y acuñando un *token envuelto* en la cadena de destino. Los puentes han sido escenario de los mayores robos de la historia del sector.

Burn (quema) — Destrucción irreversible de tokens mediante su envío a una dirección desde la que no pueden gastarse o mediante la llamada a una función del contrato que reduce la oferta. La quema se utiliza para reembolsar *tokens LP* y para retirar *stablecoins* en el momento del reembolso.

Capital markets product (producto de los mercados de capitales) — Categoría legal singapurense de la sección 2(1) de la Securities and Futures Act 2001 (SFA, ley de valores y futuros), que abarca los valores mobiliarios, las participaciones en un esquema de inversión colectiva, los contratos de derivados y determinados contratos de divisas. Un token que sea un producto de los mercados de capitales está regulado por la SFA, sea o no también un *DPT*.

CBDC — Moneda digital de banco central (central bank digital currency), es decir, un pasivo de un banco central en forma de token; su variante mayorista está restringida a entidades financieras. La variante minorista estaría a disposición del público. Suiza y Singapur han emitido CBDC mayorista en proyectos piloto, y ninguno de los dos prevé una versión minorista.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Chain (cadena) — Término coloquial para designar un registro distribuido, derivado del encadenamiento de los bloques, de modo que «on-chain» significa registrado en el registro y «off-chain» significa registrado en otro lugar, por ejemplo en los libros internos de un custodio.

Cold wallet (monedero frío) — *Monedero* cuya *clave privada* se guarda en un dispositivo que nunca se conecta a internet, de modo que la firma exige un paso manual y es imposible robar la clave a distancia. Es la contrapartida del *monedero caliente*.

Collective investment scheme (esquema de inversión colectiva) — En el Derecho suizo, patrimonio captado de inversores para su inversión colectiva y gestionado por cuenta de estos por un tercero (Ley de instituciones de inversión colectiva, KAG/LIIC, art. 7). En el Derecho singapurense, es un mecanismo en el que los partícipes carecen de control cotidiano sobre un patrimonio agrupado que se gestiona como un todo (SFA, sección 2(1)). Varias estructuras DeFi cumplen ambas definiciones.

Company limited by guarantee (CLG, sociedad limitada por garantía) — Sociedad singapurense sin capital social, regulada en la sección 17 de la Companies Act 1967, cuyos miembros se comprometen a aportar una suma simbólica en caso de liquidación. Se utiliza como envoltorio jurídico de protocolos y a menudo se la llama «fundación», aunque no lo es.

Confirmation (confirmación) — Inclusión de una transacción en un bloque, junto con cada bloque posterior que se construye sobre él, de modo que una plataforma de intercambio que exige seis confirmaciones espera cinco bloques más antes de abonar un depósito. El plazo de espera existe porque la *firmeza* en los registros públicos es probabilística.

Consensus (consenso) — Protocolo mediante el cual los participantes de un registro se ponen de acuerdo sobre el siguiente bloque sin necesidad de confiar unos en otros; la *prueba de trabajo* y la *prueba de participación* son sus dos grandes familias.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Crypto asset (criptoactivo) — Término general que este libro emplea para cualquier token registrado en un registro distribuido, y que corresponde al término legal suizo «activo criptográfico» (kryptobasierter Vermögenswert) del art. 242a de la Ley federal sobre la ejecución y la quiebra (SchKG/LP) y del art. 16 de la Ley de bancos (BankG/LB).

Custodian (custodio) — Persona que conserva las *claves privadas* que controlan los tokens de los clientes. En Singapur, se trata de un servicio de pago sujeto a licencia conforme a la Payment Services Act (PSA, ley de servicios de pago). En Suiza, convierte al titular en intermediario financiero conforme a la GwG/LBA y, posiblemente, en banco si tiene derecho a utilizar los activos.

DAO — Organización autónoma descentralizada (decentralised autonomous organisation), es decir, un grupo que gobierna un protocolo o una tesorería mediante votaciones ponderadas por tokens a través de smart contracts. Sin un envoltorio jurídico, una DAO es una *sociedad simple* según el Derecho suizo y una partnership o una asociación sin personalidad jurídica según el Derecho singapurense.

Decentralised finance (DeFi, finanzas descentralizadas) — Servicios financieros prestados por smart contracts en registros públicos sin que un intermediario custodie los activos de los clientes; el informe del Consejo Federal de 16 de diciembre de 2022 es el texto de referencia suizo.

Delegated staking (staking delegado) — *Staking* en el que el titular conserva la clave de retirada y cede a un operador únicamente el derecho de validación, a diferencia del staking en custodia, en el que el custodio conserva todas las claves.

Derivation path (ruta de derivación) — Secuencia mediante la cual una *semilla* genera pares de claves individuales conforme al estándar BIP-32, de modo que una sola semilla controla direcciones en muchas cadenas a través de rutas distintas. Por ello, un inventario de tenencias debe explorar todas las rutas habituales.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Digital payment token (DPT, token de pago digital) — Término legal singapurense de la sección 2(1) de la Payment Services Act 2019 para un token que es una representación digital de valor, no está denominado en ninguna moneda, se utiliza como medio de cambio y puede transferirse electrónicamente. Bitcoin y Ether son DPT.[2]

Digital token service provider (DTSP, proveedor de servicios de tokens digitales) — Persona que presta desde Singapur servicios de tokens digitales a clientes situados fuera de Singapur, sujeta a licencia conforme a la Parte 9 de la Financial Services and Markets Act 2022 desde el 30 de junio de 2025. La MAS ha declarado que solo concederá licencias a DTSP en circunstancias sumamente limitadas.

Digital twin (gemelo digital) — Token que representa un activo inscrito en otro registro, como inmuebles, acciones u oro. Es el otro registro el que rige la titularidad, de modo que el token es un derecho de crédito o una representación cuyo efecto depende de los acuerdos entre el titular inscrito y el titular del token.

Distributed ledger technology (DLT, tecnología de registro distribuido) — Término general para las bases de datos que muchos participantes mantienen en copias idénticas y que se actualizan por *consenso*. La Ley TRD (DLT) suiza de 25 de septiembre de 2020 emplea el término sin comprometerse con ninguna arquitectura concreta.

DLT trading facility (sistema de negociación TRD) — Categoría de licencia suiza del art. 73a y ss. de la Ley de infraestructuras del mercado financiero (FinfraG/LIMF) para un centro que admite *valores registrados* a negociación multilateral y que puede prestar también servicios de liquidación y custodia; SIX Digital Exchange es titular de la primera licencia.

E-money (dinero electrónico) — Conforme a la sección 2(1) de la Payment Services Act 2019, valor monetario almacenado electrónicamente, denominado en una moneda, pagado por adelantado, que representa un crédito frente al emisor y que terceros aceptan como medio de pago. Una stablecoin vinculada a una moneda fiduciaria que confiera un derecho de reembolso puede ser dinero electrónico.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

E-money token (EMT, token de dinero electrónico) — Categoría de MiCA, conforme al art. 3, apdo. 1, punto 7, del Reglamento (UE) 2023/1114, para un criptoactivo que mantiene un valor estable referenciándose a una única moneda oficial. En la UE, solo las entidades de crédito y las entidades de dinero electrónico pueden emitir EMT.

ERC-20 — Estándar de Ethereum para tokens fungibles, que define las funciones que debe ofrecer un contrato de token y que siguen la mayoría de los tokens de Ethereum y de las cadenas compatibles. ERC-721 y ERC-1155 son los estándares correspondientes para los *NFT*.

Exploit — Aprovechamiento de un defecto de un smart contract para extraer valor en contra del funcionamiento previsto del contrato. Si un exploit constituye robo, estafa o uso lícito de código publicado es una cuestión que abordan la Parte H, capítulo I, y la Parte N, capítulo I.

Finality (firmeza) — Momento a partir del cual una transacción ya no puede revertirse conforme a las reglas del registro; es probabilística en las cadenas de *prueba de trabajo*, económica en las cadenas de *prueba de participación* transcurrido un período definido y determinista en los *registros permisionados*.

Financial intermediary (intermediario financiero) — Término de la GwG/LBA suiza (art. 2, apdo. 3) para las personas que, a título profesional, aceptan, conservan, invierten o transfieren activos ajenos. La mayoría de los proveedores de servicios cripto que tienen poder de disposición son intermediarios financieros y deben adherirse a un organismo de autorregulación.

Flash loan (préstamo flash) — Préstamo sin garantía que se toma y se devuelve dentro de una misma transacción, la cual fracasa por completo si no se produce la devolución; se utiliza legítimamente para el arbitraje e ilegítimamente para manipular *oráculos* y vaciar protocolos.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Fork (bifurcación) — Divergencia en el historial o en las reglas de un registro: un soft fork endurece las reglas de forma compatible, mientras que un hard fork crea dos cadenas. Tras un hard fork, cada titular del token original posee la misma cantidad en ambas.

Foundation (Stiftung, fundación) — Persona jurídica suiza regulada en el art. 80 y ss. del Código Civil suizo (ZGB/CC), que se constituye afectando un patrimonio a un fin, está gobernada por un consejo y se halla bajo la supervisión de una autoridad pública. Se ha convertido en el envoltorio jurídico estándar para las tesorerías de protocolos en Zug.

Front-end — Sitio web o aplicación a través del cual los usuarios interactúan con un *smart contract*; tanto el Consejo Federal como la MAS han identificado a su operador como el destinatario natural de la regulación en DeFi.

Gas — Comisión que se paga a los validadores o mineros de un registro por procesar una transacción, denominada en el token nativo del registro. El gas es un coste de la actividad y, como tal, deducible cuando la actividad es empresarial.

Governance token (token de gobernanza) — Token que confiere derechos de voto sobre los parámetros, la tesorería o las actualizaciones de un protocolo. Su clasificación regulatoria depende de si el voto puede dirigir valor económico a los titulares y de si efectivamente lo ha hecho.

Hash — Huella de longitud fija calculada a partir de unos datos mediante una función unidireccional, de modo que cualquier cambio en los datos modifica el hash. Los hashes permiten encadenar los bloques y que cualquiera verifique la integridad de un registro.

Hot wallet (monedero caliente) — *Monedero* cuya *clave privada* reside en un sistema conectado a internet y puede firmar de inmediato; los custodios lo utilizan para disponer de un saldo operativo para retiradas y es el objetivo habitual de los robos. Es la contrapartida del *monedero frío*.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Hybrid token (token híbrido) — Token con más de una función económica, al que la FINMA aplica de forma acumulativa los requisitos de cada categoría pertinente conforme a la sección 3.1 de las Directrices sobre ICO de 16 de febrero de 2018.

Initial coin offering (ICO, oferta inicial de monedas) — Venta pública de tokens de nueva creación para financiar un proyecto; el término dominó en 2017 y 2018 y ha cedido en gran medida el paso a «token sale» o «token generation event». No obstante, las Directrices sobre ICO de la FINMA de 2018 siguen siendo la referencia suiza en materia de clasificación.

Key share (fragmento de clave) — Fragmento de una *clave privada* que conserva una de las partes en un esquema de *computación multipartita*; su distribución entre las partes determina quién tiene el control a efectos regulatorios y concursales.

Layer 2 (capa 2) — Red que procesa transacciones fuera de un registro principal y publica periódicamente en él un resumen para ganar velocidad y reducir costes, como Arbitrum, Optimism y Base en Ethereum o Lightning en Bitcoin. Los activos de una capa 2 suelen estar bloqueados en un contrato *puente* en la cadena principal.

Ledger-based security (Registerwertrecht, valor registrado) — Derecho emitido como valor en un registro distribuido que cumple los requisitos funcionales del art. 973d, apdo. 2, del Código de Obligaciones suizo (OR/CO), de modo que la inscripción en el registro y el derecho quedan fusionados. La transmisión se produce mediante inscripción en el registro. Introducido el 1 de febrero de 2021, es la única forma, en cualquiera de los dos centros, en la que el propio registro distribuido constituye el registro de un valor.[3]

Limited-purpose DPT (DPT de propósito limitado) — Exclusión singapurense de la definición de *DPT* de la sección 2(1) de la Payment Services Act 2019 para tokens utilizables únicamente dentro de un sistema cerrado, como objetos de videojuegos o puntos de fidelización. La exclusión se pierde en cuanto el token puede canjearse por dinero o por otros DPT fuera del sistema.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Liquid staking (staking líquido) — *Staking* a través de un protocolo que emite un token-recibo transferible, como stETH o rETH, que representa la posición en staking, se negocia libremente y se utiliza como garantía en todo el ecosistema DeFi.

Liquidity pool (pool de liquidez) — Smart contract que conserva los tokens depositados por los *proveedores de liquidez* para su uso por un *AMM* o un protocolo de préstamo. El análisis del capítulo VI considera que el pool contrata por cuenta de los proveedores.

Liquidity provider (LP, proveedor de liquidez) — Persona que deposita tokens en un *pool de liquidez* a cambio de *tokens LP* y de una parte de las comisiones que el pool obtiene de los operadores.

LP token (token LP) — Token que representa una participación proporcional en un *pool de liquidez*, reembolsable mediante su *quema* a cambio de la parte que corresponde al titular en los activos del pool y en las comisiones acumuladas. Entre los tokens DeFi, es el candidato más claro a ser clasificado como participación en un *esquema de inversión colectiva*.

Memecoin — Token de tipo pago sin utilidad, sin derecho frente a un emisor y sin proyecto, cuyo valor descansa en la atención de la comunidad; es un token de pago según la taxonomía de la FINMA y un *DPT* en Singapur.

Mempool — Conjunto de transacciones difundidas a una red pero aún no incluidas en un bloque. Las transacciones pendientes son visibles para todos los participantes y, por tanto, cualquiera dispuesto a pagar una comisión más alta puede adelantarse a ellas (front-running).

MiCA — Reglamento (UE) 2023/1114 relativo a los mercados de criptoactivos, aplicable a las stablecoins desde el 30 de junio de 2024 y a los demás criptoactivos y proveedores de servicios desde el 30 de diciembre de 2024. No se aplica en Suiza ni en Singapur, pero rige para las contrapartes de ambos centros en la UE.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Miner (minero) — Participante de una red de *prueba de trabajo* que invierte capacidad de cálculo para proponer bloques y obtiene a cambio nuevos tokens y comisiones. Los rendimientos de la minería tributan como renta en ambos centros cuando la actividad tiene carácter empresarial.

Mint (acuñación) — Creación de nuevos tokens mediante una función del contrato; así se emiten las stablecoins, se crean los *tokens envueltos* y se generan los *tokens LP* cuando se deposita liquidez.

Multi-party computation (MPC, computación multipartita) — Técnica criptográfica mediante la cual varias partes que poseen *fragmentos de clave* generan conjuntamente una firma sin que ninguna llegue a conocer nunca la *clave privada* completa; la utilizan hoy la mayoría de las plataformas de custodia institucional.

Multi-signature (multisig, multifirma) — Dirección configurada en el propio registro de modo que un umbral de varias claves, por ejemplo dos de tres, debe firmar cualquier transacción. La *MPC* logra un resultado similar off-chain.

Node (nodo) — Ordenador que ejecuta el software del registro y conserva una copia de este; los nodos completos verifican todas las transacciones, mientras que los *validadores* y los *mineros* son nodos que además proponen bloques.

Non-fungible token (NFT, token no fungible) — Token cuyo contrato registra un identificador único para cada unidad, de modo que las unidades son distinguibles entre sí. La clasificación sigue al derecho representado. Los NFT únicos quedan por lo general fuera de la regulación financiera en ambos centros, mientras que los NFT en serie o fraccionados pueden quedar comprendidos en ella.

Omnibus wallet (monedero ómnibus) — Modalidad de custodia en la que un *custodio* conserva los tokens de muchos clientes en una o unas pocas direcciones y los derechos de los clientes figuran únicamente en sus libros, a diferencia del *monedero segregado*. El Derecho suizo protege a los clientes de cuentas ómnibus en caso de insolvencia si sus participaciones son «fácilmente atribuibles» conforme al art. 242a SchKG/LP.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Oracle (oráculo) — Servicio, cuyo proveedor dominante es Chainlink, que suministra datos externos, como precios, a los *smart contracts*. El fallo o la manipulación de oráculos es una de las principales causas de pérdidas en DeFi y una cuestión de responsabilidad recurrente.

Payment token (token de pago) — Categoría de la FINMA para tokens destinados a servir como medio de pago o de transferencia de valor sin derecho alguno frente a un emisor, como Bitcoin y Ether. Su emisión está sujeta a la GwG/LBA, pero queda fuera del Derecho del mercado de valores.

Perpetual future (perp, futuro perpetuo) — Contrato de futuros sin vencimiento que se mantiene alineado con el precio al contado mediante pagos de financiación (funding) entre las posiciones largas y cortas; es un derivado tanto en el Derecho suizo como en el singapurense.

Permissioned ledger (registro permisionado) — Registro cuyos nodos son entidades conocidas y previamente autorizadas, como en los consorcios bancarios y en la mayoría de los proyectos piloto de tokenización. Ofrece *firmeza* determinista y operadores identificables, a diferencia de los registros públicos o sin permisos como Bitcoin y Ethereum.

Points (puntos) — Cómputos off-chain que lleva un proyecto para registrar la actividad de los usuarios y que se espera que se conviertan en tokens en un lanzamiento futuro. Los puntos quedan fuera de toda taxonomía regulatoria, pero pueden dar lugar a reclamaciones por declaraciones engañosas.

Private key (clave privada) — Número aleatorio de gran tamaño que permite a su titular firmar transacciones que mueven tokens desde la *dirección* correspondiente. La clave privada es el único hecho que confiere poder de disposición fáctico sobre un token y constituye el fundamento de todo análisis de custodia e insolvencia en este libro.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Proof of stake (prueba de participación) — Mecanismo de *consenso* en el que los *validadores* bloquean tokens como fianza y son seleccionados para proponer bloques en proporción a su participación, y en el que la conducta indebida se sanciona mediante *slashing*. Ethereum utiliza la prueba de participación desde septiembre de 2022.

Proof of work (prueba de trabajo) — Mecanismo de *consenso*, utilizado por Bitcoin, en el que los *mineros* compiten por resolver un problema computacional para obtener el derecho a proponer un bloque y la recompensa asociada.

Protocol (protocolo) — Conjunto de reglas y smart contracts que constituyen un servicio DeFi o una red blockchain. Un protocolo no es una persona, y si hay una persona detrás de él es la cuestión regulatoria central de los capítulos VI y VII.

Public key (clave pública) — Valor derivado de una *clave privada* mediante una función unidireccional, del que a su vez se deriva la *dirección*, y que permite a cualquiera verificar una firma sin conocer la clave privada.

Purpose-bound money (PBM, dinero de finalidad vinculada) — Concepto de diseño singapurense publicado por la MAS en junio de 2023, en el que un token de dinero digital se envuelve en una capa programable que restringe cómo y dónde puede gastarse. La restricción es contractual y no afecta al dinero subyacente.

Readily attributable (fácilmente atribuible) — Criterio del art. 242a, apdo. 2, letra b, SchKG/LP para la entrega a los clientes de criptoactivos agrupados en la quiebra de un custodio suizo. Se cumple cuando los registros del custodio muestran la participación de cada cliente sin necesidad de reconstrucción.

Registration agreement (acuerdo de registro) — Acuerdo del art. 973d, apdo. 1, OR/CO mediante el cual las partes de un derecho convienen en que este se emita como *valor registrado* en un registro determinado. El acuerdo debe constar en el registro o estar vinculado a él y debería definir qué cadena es «el registro» tras una *bifurcación*.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Rehypothecation (rehipotecación) — Utilización por un *custodio* de los activos de los clientes para sus propios fines, como prestarlos o pignorarlos, lo que pone fin a la custodia y convierte al cliente en acreedor ordinario sin garantía en ambos centros.

Restaking — Afectación de tokens ya en staking o de recibos de *staking líquido* como garantía de servicios adicionales, con la obtención de recompensas adicionales y la asunción de un riesgo adicional de *slashing*; lo introdujo EigenLayer en 2023 y 2024.

Rollup — Tipo de *capa 2* que ejecuta transacciones off-chain y publica en la cadena principal datos comprimidos o pruebas de validez; los optimistic rollups permiten impugnaciones y los zero-knowledge rollups publican pruebas criptográficas.

Seed phrase (frase semilla) — Secuencia de doce o veinticuatro palabras que codifica la *semilla* de la que un monedero deriva todas sus *claves privadas* conforme al estándar BIP-39. Quien posee la frase semilla controla todas las direcciones derivadas de ella.

Segregated wallet (monedero segregado) — Modalidad de custodia en la que los tokens de cada cliente se conservan en una *dirección* separada controlada por el *custodio*. Es la contrapartida del *monedero ómnibus* y produce el resultado más limpio en caso de insolvencia en ambos centros.

Simple partnership (einfache Gesellschaft, sociedad simple) — Forma residual suiza del art. 530 y ss. OR/CO para personas que persiguen un fin común con medios comunes sin adoptar otra forma jurídica, y en la que los socios responden solidaria e ilimitadamente. Es la calificación por defecto de una *DAO* sin envoltorio jurídico.

Single-currency stablecoin (SCS, stablecoin de moneda única) — Categoría regulatoria de la MAS, anunciada el 15 de agosto de 2023, para una stablecoin vinculada al dólar de Singapur o a una moneda del G10 y emitida en Singapur con sujeción a requisitos de reservas, capital, reembolso y divulgación de información. Solo los emisores que los cumplan pueden utilizar la denominación «MAS-regulated stablecoin».

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Slashing — Destrucción de una parte de los tokens en staking de un *validador* como sanción por conducta indebida o por inactividad en la *prueba de participación*; es un riesgo que los custodios que ofrecen *staking* deben comunicar y gestionar.

Smart contract — Programa almacenado en un registro que se ejecuta cuando una transacción lo invoca; es una herramienta de ejecución y no constituye por sí mismo un contrato en sentido jurídico. Si existe un contrato jurídico entre las partes que interactúan con él se determina conforme al Derecho contractual ordinario.

Soulbound token — *NFT* intransferible vinculado a una dirección y utilizado como credencial o certificación; queda fuera de todas las taxonomías financieras porque no puede negociarse ni utilizarse como medio de pago.

Stablecoin — Token diseñado para mantener un valor constante respecto de una referencia, normalmente una moneda fiduciaria; el capítulo IV lo clasifica, según la promesa de reembolso que lo respalda, como respaldado por moneda fiduciaria, respaldado por criptoactivos o algorítmico.

Staking — Afectación de tokens a una red de *prueba de participación* para obtener recompensas de validación, mediante modelos que van desde el staking individual, pasando por el *delegado* y el custodiado, hasta el *staking líquido*. La Comunicación de la FINMA 08/2023, de 20 de diciembre de 2023, fija las condiciones suizas para el staking en custodia.

Token — Unidad de valor o de derecho registrada en un registro distribuido; este libro emplea el término para cualquier unidad de este tipo y reserva «criptoactivo» y «activo digital» para la categoría general.

Total value locked (TVL, valor total bloqueado) — Valor agregado de los activos depositados en un protocolo DeFi o en el conjunto del sector; mide la escala y no dice nada sobre la seguridad.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Travel rule (regla de viaje) — Requisito del GAFI (FATF), aplicado en Suiza mediante el art. 10 de la Ordenanza de la FINMA sobre el blanqueo de capitales (GwV-FINMA/OBA-FINMA) y en Singapur mediante la MAS Notice PSN02, según el cual la información sobre el ordenante y el beneficiario debe acompañar las transferencias de criptoactivos entre intermediarios regulados.

Unhosted wallet (monedero no alojado) — *Monedero* controlado por su usuario y no por un intermediario regulado, también llamado monedero autoalojado o privado. Las transferencias desde y hacia monederos no alojados están sujetas en ambos centros a requisitos específicos de la regla de viaje y de diligencia debida.

Utility token (token de utilidad) — Categoría de la FINMA para un token que proporciona acceso digital a una aplicación o a un servicio. Queda fuera del Derecho del mercado de valores si el servicio existe en el momento de la venta. La FINMA lo trata como *token de inversión* si se vende para financiar un servicio que aún no está operativo.

UTXO model (modelo UTXO) — Diseño de registro, utilizado por Bitcoin, en el que el valor se sigue como salidas de transacción no gastadas (unspent transaction outputs) independientes, cada una de las cuales se gasta íntegramente y se sustituye por nuevas salidas. A diferencia del *modelo de cuentas*, permite un rastreo basado en el linaje.

Validator (validador) — Participante de una red de *prueba de participación* que propone y certifica bloques tras bloquear tokens como fianza, y que obtiene recompensas por su participación honesta y se expone al *slashing* en caso de conducta indebida.

Wallet (monedero) — Software o hardware que almacena *claves privadas* y firma transacciones; en él no se almacena nada salvo las claves, porque los tokens permanecen en el registro.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

White paper (libro blanco) — Documento que describe un proyecto de token, su tecnología y su economía. Con arreglo a MiCA, es un documento de información regulado. Con arreglo a la Ley de servicios financieros suiza (FIDLEG/LSFin) y a la SFA, puede constituir un folleto si el token es un valor y no se aplica ninguna exención.

Wrapped token (token envuelto) — Token de un registro que representa un token bloqueado en otro a través de un *puente*, cuyo ejemplo principal es WBTC; económicamente es un derecho de crédito frente a quien controle el activo bloqueado.

Zero-knowledge proof (prueba de conocimiento cero) — Método criptográfico mediante el cual una parte demuestra que una afirmación es cierta sin revelar los datos subyacentes. Se utiliza en los *rollups* para la escalabilidad y en los sistemas de identidad para acreditar atributos como la edad o la jurisdicción sin revelar la identidad. Las Partes F y L analizan su relevancia para el diseño del cumplimiento normativo en materia de prevención del blanqueo de capitales.

Notas

1. Anti-Money Laundering Act (GwG/LBA), SR 955.0, art. 2, apdo. 3 (intermediarios financieros del sector no bancario). Parte F, capítulo I. ↩
2. Payment Services Act 2019 (Singapur), sección 2(1). La definición excluye el *dinero electrónico* y los *DPT de propósito limitado*. Parte K, capítulo I. ↩
3. Código de Obligaciones suizo (OR/CO), SR 220, arts. 973d–973i. Parte D, capítulo III. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.