Glossaire des termes techniques utilisés dans cet ouvrage

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

Les entrées suivantes définissent, par ordre alphabétique (selon le terme anglais), les termes techniques employés dans l'ouvrage, dans le sens que celui-ci leur donne. Lorsqu'un terme fait l'objet d'une définition légale en droit suisse ou singapourien, l'entrée le signale et en indique la source. Lorsque techniciens et juristes emploient un terme différemment, l'entrée retient l'usage juridique adopté ici. Les renvois à d'autres entrées figurent en italique.

Modèle à comptes (account model) — Architecture de registre dans laquelle chaque adresse porte un solde qui augmente et diminue au gré des transactions, comme sur Ethereum, par opposition au *modèle UTXO* utilisé par Bitcoin. La distinction influe sur la manière dont les tribunaux retracent les fonds et dont les dépositaires attribuent les avoirs de clients mis en commun.

Adresse (address) — Chaîne de caractères dérivée d'une *clé publique* qui identifie une destination pour des jetons sur un registre, que chacun peut créer gratuitement et qui ne porte aucun nom. Une adresse devient une donnée personnelle au sens du droit suisse et singapourien de la protection des données dès qu'elle peut être rattachée à une personne physique.

© 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 — Distribution gratuite de jetons à des adresses existantes, généralement pour récompenser les premiers utilisateurs ou élargir la répartition des avoirs. Les airdrops ont des conséquences fiscales, en tant que revenu ou en tant qu'acquisition à coût nul, selon que le bénéficiaire a le statut de commerçant professionnel ou d'investisseur privé.

Stablecoin algorithmique (algorithmic stablecoin) — Jeton qui tente de maintenir une valeur stable par des ajustements de l'offre sans couverture intégrale, dont l'UST de Terraform était l'exemple principal jusqu'à son effondrement en mai 2022. Ni la FINMA ni la MAS ne traitent ces jetons comme des stablecoins sur le plan réglementaire.

LBA (AMLA) — La loi fédérale suisse concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (loi sur le blanchiment d'argent, LBA), RS 955.0, qui s'applique aux *intermédiaires financiers* et que la FINMA interprète comme couvrant la plupart des prestataires disposant d'un pouvoir de disposition sur les cryptoactifs de leurs clients.[1]

Jeton se référant à un ou des actifs (asset-referenced token, ART) — Catégorie de MiCA, au sens du règlement (UE) 2023/1114, art. 3, par. 1, point 6, désignant un crypto-actif qui vise à maintenir une valeur stable en se référant à une autre valeur ou à un autre droit, ou à une combinaison de ceux-ci, y compris plusieurs monnaies. Il est le pendant du *jeton de monnaie électronique* à monnaie unique.

Jeton d'investissement (asset token) — Catégorie de la FINMA désignant un jeton qui représente une créance ou un droit de participation, une part de bénéfices futurs ou un droit sur un actif, au sens du chiffre 3.1 du guide pratique ICO du 16 février 2018. Ces jetons sont, dans presque tous les cas, des valeurs mobilières en droit suisse et entraînent des conséquences en matière de prospectus et d'autorisation.

Teneur de marché automatisé (automated market maker, AMM) — Plateforme d'échange décentralisée, dont Uniswap est l'exemple principal, qui fixe le prix des transactions par une formule appliquée à une liquidité mise en commun,

© 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.

sans rapprocher des ordres d'achat et de vente. Selon l'analyse du chapitre VI, la contrepartie d'une transaction sur un AMM est l'ensemble des *fournisseurs de liquidité* du pool.

Bloc (block) — Lot de transactions ajouté en une seule unité à un registre et portant le *hash* du bloc précédent, de sorte que les blocs forment une chaîne dont toute modification est décelable par chacun.

Explorateur de blocs (block explorer) — Site web, tel qu'Etherscan ou mempool.space, qui affiche sous une forme lisible le contenu d'un registre public. Un juriste devrait savoir lire une transaction sur un explorateur de blocs avant d'émettre le moindre avis à son sujet.

Pont (bridge) — Mécanisme permettant de représenter un jeton d'un registre sur un autre, généralement en bloquant l'original dans un contrat et en émettant un *jeton enveloppé* sur la chaîne de destination. Les ponts ont été le théâtre des plus grands vols de l'histoire du secteur.

Destruction (burn) — Destruction irréversible de jetons, par leur envoi à une adresse depuis laquelle ils ne peuvent plus être dépensés ou par l'appel d'une fonction du contrat qui réduit l'offre. La destruction sert à racheter des *jetons LP* et à retirer des *stablecoins* lors de leur remboursement.

Capital markets product — Catégorie légale singapourienne de la section 2(1) du Securities and Futures Act 2001 (SFA, loi sur les valeurs mobilières et les contrats à terme), qui couvre les valeurs mobilières, les parts de placements collectifs, les contrats dérivés et certains contrats de change. Un jeton qui est un capital markets product est régi par le SFA, qu'il soit ou non également un *DPT*.

MNBC (CBDC) — Monnaie numérique de banque centrale, c'est-à-dire un engagement d'une banque centrale sous forme de jeton, dont la variante de gros est réservée aux établissements financiers. La variante de détail serait accessible au public. La Suisse et Singapour ont toutes deux émis une MNBC de gros dans le cadre de projets pilotes, et aucune ne prévoit de version de détail.

© 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.

Chaîne (chain) — Terme courant désignant un registre distribué, tiré de l'enchaînement des blocs. « On-chain » signifie ainsi inscrit sur le registre, et « off-chain » inscrit ailleurs, par exemple dans les livres internes d'un dépositaire.

Portefeuille froid (cold wallet) — *Portefeuille* dont la *clé privée* est conservée sur un appareil jamais connecté à internet, de sorte que la signature exige une intervention manuelle et que le vol de la clé à distance est impossible. Il est le pendant du *portefeuille chaud*.

Placement collectif (collective investment scheme) — En droit suisse, apports constitués par des investisseurs pour être gérés collectivement pour leur compte par un tiers (LPCC, art. 7). En droit singapourien, dispositif dans lequel les participants n'exercent pas de contrôle courant sur des biens mis en commun et gérés comme un tout (SFA, section 2(1)). Plusieurs structures DeFi répondent aux deux définitions.

Company limited by guarantee (CLG) — Société singapourienne sans capital social, régie par la section 17 du Companies Act 1967, dont les membres s'engagent à verser une somme symbolique en cas de liquidation. Elle sert d'enveloppe juridique aux protocoles et est souvent appelée « fondation », ce qu'elle n'est pas.

Confirmation — Inclusion d'une transaction dans un bloc, ainsi que chaque bloc ultérieur qui s'appuie sur celui-ci. Une plateforme exigeant six confirmations attend donc cinq blocs supplémentaires avant de créditer un dépôt. Ce délai d'attente existe parce que la *finalité* sur les registres publics est probabiliste.

Consensus — Protocole par lequel les participants au registre s'accordent sur le bloc suivant sans se faire mutuellement confiance, dont la *preuve de travail* et la *preuve d'enjeu* sont les deux grandes familles.

Crypto-actif (crypto asset) — Terme général employé dans cet ouvrage pour tout jeton inscrit sur un registre distribué. Il correspond au terme légal suisse de « cryptoactifs » (kryptobasierte Vermögenswerte) figurant à l'art. 242a LP et à l'art. 16 LB.

© 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.

Dépositaire (custodian) — Personne qui détient les *clés privées* contrôlant les jetons de ses clients. À Singapour, il s'agit d'un service de paiement soumis à licence en vertu du Payment Services Act (PSA, loi sur les services de paiement). En Suisse, cette activité fait de son titulaire un intermédiaire financier au sens de la LBA, voire une banque s'il dispose d'un droit d'utiliser les avoirs.

DAO — Organisation autonome décentralisée (decentralised autonomous organisation), c'est-à-dire un groupe qui gouverne un protocole ou une trésorerie par un vote pondéré en fonction des jetons détenus, au moyen de smart contracts. Sans enveloppe juridique, une DAO est une *société simple* en droit suisse et une partnership ou une unincorporated association en droit singapourien.

Finance décentralisée (decentralised finance, DeFi) — Services financiers fournis par des smart contracts sur des registres publics sans intermédiaire détenant les avoirs des clients. Le rapport du Conseil fédéral du 16 décembre 2022 en est le texte de référence suisse.

Staking délégué (delegated staking) — *Staking* dans lequel le détenteur conserve la clé de retrait et ne cède à un opérateur que le droit de validation, par opposition au staking en dépôt, dans lequel le dépositaire détient toutes les clés.

Chemin de dérivation (derivation path) — Séquence par laquelle une *seed* génère des paires de clés individuelles selon la norme BIP-32, de sorte qu'une seule seed contrôle des adresses sur de nombreuses chaînes par des chemins différents. Un inventaire des avoirs doit donc balayer tous les chemins usuels.

Digital payment token (DPT) — Terme légal singapourien de la section 2(1) du Payment Services Act 2019 (« jeton de paiement numérique ») désignant un jeton qui constitue une représentation numérique de valeur, n'est libellé dans aucune monnaie, sert de moyen d'échange et peut être transféré électroniquement. Le bitcoin et l'ether sont des DPT.[2]

© 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 token service provider (DTSP) — Personne fournissant depuis Singapour des services de jetons numériques à des clients situés hors de Singapour, soumise à licence en vertu de la partie 9 du Financial Services and Markets Act 2022 (FSMA) depuis le 30 juin 2025. La MAS a déclaré qu'elle n'accorderait de licence aux DTSP que dans des circonstances extrêmement limitées.

Jumeau numérique (digital twin) — Jeton qui représente un actif inscrit dans un autre registre, par exemple un bien foncier, des actions ou de l'or. C'est cet autre registre qui régit la propriété : le jeton est donc une créance ou une représentation dont l'effet dépend des arrangements entre le propriétaire inscrit et le détenteur du jeton.

Technologie des registres distribués (distributed ledger technology, DLT) — Terme général désignant des bases de données détenues en copies identiques par de nombreux participants et mises à jour par *consensus*. La loi TRD suisse du 25 septembre 2020 emploie ce terme sans s'attacher à une architecture particulière.

Système de négociation fondé sur la TRD (DLT trading facility) — Catégorie d'autorisation suisse au sens des art. 73a ss LIMF, désignant une plateforme qui admet des *droits-valeurs inscrits* au négoce multilatéral et peut aussi assurer le règlement et la garde. SIX Digital Exchange a obtenu la première autorisation de ce type.

Monnaie électronique (e-money) — Au sens de la section 2(1) du Payment Services Act 2019, valeur monétaire stockée électroniquement, libellée dans une monnaie, payée d'avance, représentant une créance sur l'émetteur et acceptée en paiement par des tiers. Un stablecoin adossé à une monnaie fiduciaire qui confère un droit au remboursement peut constituer de la monnaie électronique.

Jeton de monnaie électronique (e-money token, EMT) — Catégorie de MiCA, au sens du règlement (UE) 2023/1114, art. 3, par. 1, point 7, désignant un crypto-actif qui vise à maintenir une valeur stable en se référant à une seule monnaie officielle. Dans l'UE, seuls les établissements de crédit et les établissements de monnaie électronique peuvent émettre des EMT.

© 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.

ERC-20 — Norme Ethereum applicable aux jetons fongibles, qui définit les fonctions qu'un contrat de jeton doit exposer et que suivent la plupart des jetons sur Ethereum et sur les chaînes compatibles. ERC-721 et ERC-1155 sont les normes correspondantes pour les *NFT*.

Exploit — Utilisation d'un défaut d'un smart contract pour en extraire de la valeur contrairement au fonctionnement voulu du contrat. La question de savoir si un exploit constitue un vol, une escroquerie ou une utilisation licite d'un code publié est traitée dans la partie H, chapitre I, et dans la partie N, chapitre I.

Finalité (finality) — Moment à partir duquel une transaction ne peut plus être annulée selon les règles du registre. Elle est probabiliste sur les chaînes à *preuve de travail*, économique sur les chaînes à *preuve d'enjeu* après un délai défini et déterministe sur les *registres permissionnés*.

Intermédiaire financier (financial intermediary) — Terme de la LBA suisse (art. 2, al. 3) désignant les personnes qui, à titre professionnel, acceptent, gardent, placent ou transfèrent des valeurs patrimoniales appartenant à des tiers. La plupart des prestataires de services crypto qui disposent d'un pouvoir de disposition sont des intermédiaires financiers et doivent s'affilier à un organisme d'autorégulation.

Prêt flash (flash loan) — Prêt sans garantie contracté et remboursé au sein d'une seule transaction, qui échoue intégralement si le remboursement n'a pas lieu. Il est utilisé de manière légitime pour l'arbitrage et de manière illégitime pour manipuler des *oracles* et vider des protocoles.

Fork — Divergence dans l'historique ou les règles d'un registre. Un soft fork durcit les règles de manière compatible, tandis qu'un hard fork crée deux chaînes. Après un hard fork, chaque détenteur du jeton d'origine en détient une quantité égale sur les deux chaînes.

Fondation (foundation) — Personne morale suisse régie par les art. 80 ss du Code civil, constituée par l'affectation de biens à un but, administrée par un conseil de fondation et placée sous la surveillance d'une autorité publique. Elle est devenue l'enveloppe juridique standard des trésoreries de protocoles à Zoug.

© 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.

Interface (front-end) — Site web ou application par lequel les utilisateurs interagissent avec un *smart contract*. Le Conseil fédéral comme la MAS ont désigné son exploitant comme le destinataire naturel de la réglementation dans la DeFi.

Gas — Frais versés aux validateurs ou aux mineurs d'un registre pour le traitement d'une transaction, libellés dans le jeton natif du registre. Le gas est un coût d'exploitation, déductible comme tel lorsque l'activité est commerciale.

Jeton de gouvernance (governance token) — Jeton conférant des droits de vote sur les paramètres, la trésorerie ou les mises à niveau d'un protocole. Sa qualification réglementaire dépend de la question de savoir si le vote peut diriger une valeur économique vers les détenteurs et s'il l'a effectivement fait.

Hash — Empreinte de longueur fixe calculée à partir de données par une fonction à sens unique, de sorte que toute modification des données modifie le hash. Les hashs permettent d'enchaîner les blocs et à chacun de vérifier l'intégrité d'un registre.

Portefeuille chaud (hot wallet) — *Portefeuille* dont la *clé privée* se trouve sur un système connecté à internet et peut signer immédiatement. Les dépositaires l'utilisent pour une réserve destinée aux retraits, et il est la cible habituelle des vols. Il est le pendant du *portefeuille froid*.

Jeton hybride (hybrid token) — Jeton remplissant plusieurs fonctions économiques, auquel la FINMA applique cumulativement les exigences de chaque catégorie pertinente, au sens du chiffre 3.1 du guide pratique ICO du 16 février 2018.

Initial coin offering (ICO) — Vente publique de jetons nouvellement créés afin de financer un projet. Le terme, omniprésent en 2017 et 2018, a largement cédé la place à « token sale » ou « token generation event ». Le guide pratique ICO de la FINMA de 2018 reste néanmoins la référence suisse en matière de qualification.

Fragment de clé (key share) — Fragment d'une *clé privée* détenu par une partie dans un dispositif de *calcul multipartite*. Sa répartition entre les parties détermine qui exerce le contrôle aux fins du droit de la surveillance et du droit de la faillite.

© 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.

Layer 2 — Réseau qui traite des transactions en dehors d'un registre principal et y publie périodiquement un récapitulatif, pour gagner en rapidité et en coût, tel qu'Arbitrum, Optimism et Base sur Ethereum ou Lightning sur Bitcoin. Les actifs d'un layer 2 sont généralement bloqués dans un contrat de *pont* sur la chaîne principale.

Droit-valeur inscrit (ledger-based security, Registerwertrecht) — Droit émis comme valeur mobilière sur un registre distribué qui satisfait aux exigences fonctionnelles de l'art. 973d, al. 2, CO, de sorte que l'inscription au registre et le droit sont indissociables. Le transfert s'opère par inscription au registre. Introduit le 1er février 2021, c'est la seule forme, dans l'une ou l'autre place, où le registre constitue lui-même le registre d'une valeur mobilière.[3]

DPT à usage limité (limited-purpose DPT) — Exclusion singapourienne de la définition du *DPT* figurant à la section 2(1) du Payment Services Act 2019, visant les jetons utilisables uniquement au sein d'un système fermé, tels que des objets de jeu ou des points de fidélité. L'exclusion tombe dès que le jeton peut être échangé contre de l'argent ou d'autres DPT en dehors du système.

Liquid staking — *Staking* effectué par l'intermédiaire d'un protocole qui émet un jeton de reçu transférable, tel que stETH ou rETH, représentant la position mise en jeu. Ce jeton se négocie librement et sert de garantie dans l'ensemble de la DeFi.

Pool de liquidité (liquidity pool) — Smart contract détenant des jetons déposés par des *fournisseurs de liquidité* pour être utilisés par un *AMM* ou un protocole de prêt. L'analyse du chapitre VI considère que le pool contracte pour le compte des fournisseurs.

Fournisseur de liquidité (liquidity provider, LP) — Personne qui dépose des jetons dans un *pool de liquidité* en échange de *jetons LP* et d'une part des frais que le pool perçoit auprès des traders.

© 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.

Jeton LP (LP token) — Jeton représentant une part proportionnelle d'un *pool de liquidité*, remboursable par *destruction* contre la part du détenteur dans les actifs et les frais accumulés du pool. C'est, parmi les jetons DeFi, le candidat le plus évident à la qualification de part d'un *placement collectif*.

Memecoin — Jeton de type paiement dépourvu d'utilité, de créance contre un émetteur et de projet, dont la valeur repose sur l'attention de la communauté. Il constitue un jeton de paiement selon la typologie de la FINMA et un *DPT* à Singapour.

Mempool — Ensemble des transactions diffusées sur un réseau mais pas encore incluses dans un bloc. Les transactions en attente sont visibles de tous les participants et peuvent donc faire l'objet d'un front-running par quiconque est prêt à payer des frais plus élevés.

MiCA — Règlement (UE) 2023/1114 sur les marchés de crypto-actifs, applicable aux stablecoins depuis le 30 juin 2024 et aux autres crypto-actifs et prestataires de services depuis le 30 décembre 2024. Il ne s'applique ni en Suisse ni à Singapour, mais régit les contreparties européennes des deux places.

Mineur (miner) — Participant à un réseau à *preuve de travail* qui consacre de la puissance de calcul à la proposition de blocs et perçoit en contrepartie de nouveaux jetons et des frais. Les revenus du minage sont imposables comme revenu dans les deux places lorsque l'activité est commerciale.

Émission (mint) — Création de nouveaux jetons par une fonction du contrat. C'est ainsi que les stablecoins sont émis, que les *jetons enveloppés* sont créés et que les *jetons LP* sont générés lors du dépôt de liquidité.

Calcul multipartite (multi-party computation, MPC) — Technique cryptographique par laquelle plusieurs parties détenant des *fragments de clé* produisent conjointement une signature sans qu'aucune d'elles ne connaisse jamais la *clé privée* entière. La plupart des plateformes de garde institutionnelle l'utilisent aujourd'hui.

© 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.

Multisignature (multisig) — Adresse configurée sur le registre lui-même de telle sorte qu'un seuil de plusieurs clés, par exemple deux sur trois, doit signer toute transaction. Le *MPC* aboutit à un résultat comparable off-chain.

Nœud (node) — Ordinateur qui exécute le logiciel du registre et en détient une copie. Les nœuds complets vérifient toutes les transactions, tandis que les *validateurs* et les *mineurs* sont des nœuds qui proposent en outre des blocs.

Jeton non fongible (non-fungible token, NFT) — Jeton dont le contrat enregistre un identifiant unique pour chaque unité, de sorte que les unités sont distinguables. La qualification suit le droit représenté. Les NFT uniques échappent en général à la réglementation financière dans les deux places, alors que les NFT de série ou fractionnés peuvent y être soumis.

Portefeuille omnibus (omnibus wallet) — Dispositif de garde dans lequel un *dépositaire* détient les jetons de nombreux clients sur une ou quelques adresses, les droits des clients n'étant enregistrés que dans ses propres livres, à la différence d'un *portefeuille ségrégué*. Le droit suisse protège les clients omnibus en cas de faillite si leurs parts peuvent être « attribuées en tout temps » au sens de l'art. 242a LP.

Oracle — Service, dont Chainlink est le fournisseur dominant, qui fournit des données externes, telles que des prix, aux *smart contracts*. La défaillance ou la manipulation d'un oracle est l'une des principales causes de pertes dans la DeFi et une question de responsabilité récurrente.

Jeton de paiement (payment token) — Catégorie de la FINMA désignant les jetons destinés à servir de moyen de paiement ou de transfert de valeur, sans créance contre un émetteur, tels que le bitcoin et l'ether. Leur émission est soumise à la LBA mais échappe au droit des valeurs mobilières.

Contrat à terme perpétuel (perpetual future, perp) — Contrat à terme sans échéance, maintenu aligné sur le prix au comptant par des paiements de financement entre détenteurs de positions longues et courtes. C'est un dérivé tant en droit suisse qu'en droit singapourien.

© 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.

Registre permissionné (permissioned ledger) — Registre dont les nœuds sont des entités connues et préalablement agréées, comme dans les consortiums bancaires et la plupart des projets pilotes de tokenisation. Il offre une *finalité* déterministe et des opérateurs identifiables, à la différence des registres publics ou sans permission tels que Bitcoin et Ethereum.

Points — Décomptes off-chain tenus par un projet, qui enregistrent l'activité des utilisateurs et sont censés être convertis en jetons lors d'un lancement futur. Les points échappent à toute typologie réglementaire, mais peuvent donner lieu à des actions pour déclarations trompeuses.

Clé privée (private key) — Grand nombre aléatoire qui permet à son détenteur de signer des transactions transférant des jetons depuis l'*adresse* correspondante. La clé privée est le seul élément qui confère un pouvoir de disposition de fait sur un jeton. Elle est le fondement de toutes les analyses de garde et de faillite de cet ouvrage.

Preuve d'enjeu (proof of stake) — Mécanisme de *consensus* dans lequel les *validateurs* bloquent des jetons à titre de caution et sont sélectionnés pour proposer des blocs en proportion de leur mise, les manquements étant sanctionnés par le *slashing*. Ethereum utilise la preuve d'enjeu depuis septembre 2022.

Preuve de travail (proof of work) — Mécanisme de *consensus*, utilisé par Bitcoin, dans lequel les *mineurs* rivalisent pour résoudre un problème de calcul afin d'obtenir le droit de proposer un bloc et de percevoir la récompense correspondante.

Protocole (protocol) — Ensemble de règles et de smart contracts qui constituent un service DeFi ou un réseau blockchain. Un protocole n'est pas une personne. La question de savoir si une personne se tient derrière lui est la question réglementaire centrale des chapitres VI et VII.

Clé publique (public key) — Valeur dérivée d'une *clé privée* par une fonction à sens unique, dont l'*adresse* est à son tour dérivée. Elle permet à chacun de vérifier une signature sans connaître la clé privée.

© 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.

Purpose-bound money (PBM) — Concept singapourien publié par la MAS en juin 2023 (« monnaie à finalité déterminée »), dans lequel un jeton de monnaie numérique est enveloppé dans une couche programmable qui restreint la manière et le lieu où il peut être dépensé. La restriction est contractuelle et la monnaie sous-jacente n'en est pas affectée.

Attribuable en tout temps (readily attributable) — Critère de l'art. 242a, al. 2, let. b, LP pour la distraction en faveur des clients de cryptoactifs mis en commun lors de la faillite d'un dépositaire suisse. Il est rempli lorsque les registres du dépositaire font apparaître la part de chaque client sans reconstitution.

Convention d'inscription (registration agreement) — Convention au sens de l'art. 973d, al. 1, CO par laquelle les parties à un droit conviennent que celui-ci sera émis comme *droit-valeur inscrit* sur un registre déterminé. La convention doit être consignée dans le registre ou reliée à celui-ci et devrait préciser quelle chaîne constitue « le registre » après un *fork*.

Réutilisation des garanties (rehypothecation) — Utilisation par un *dépositaire* des avoirs de ses clients à ses propres fins, par exemple en les prêtant ou en les nantissant. Elle met fin à la garde et transforme le client en créancier chirographaire dans les deux places.

Restaking — Engagement de jetons déjà mis en jeu ou de reçus de *liquid staking* comme garantie au profit de services supplémentaires, procurant des récompenses supplémentaires et comportant un risque de *slashing* supplémentaire. EigenLayer l'a introduit en 2023 et 2024.

Rollup — Type de *layer 2* qui exécute les transactions off-chain et publie sur la chaîne principale des données compressées ou des preuves de validité. Les rollups optimistes admettent des contestations, tandis que les rollups à divulgation nulle de connaissance publient des preuves cryptographiques.

© 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.

Phrase de récupération (seed phrase) — Suite de douze ou vingt-quatre mots encodant la *seed* à partir de laquelle un portefeuille dérive toutes ses *clés privées* selon la norme BIP-39. Quiconque détient la phrase de récupération contrôle toutes les adresses qui en sont dérivées.

Portefeuille ségrégué (segregated wallet) — Dispositif de garde dans lequel les jetons de chaque client sont détenus sur une *adresse* distincte contrôlée par le *dépositaire*. Il est le pendant du *portefeuille omnibus* et produit le résultat le plus net en cas de faillite dans les deux places.

Société simple (simple partnership, einfache Gesellschaft) — Forme suisse subsidiaire, régie par les art. 530 ss CO, applicable aux personnes qui poursuivent un but commun avec des moyens communs sans adopter une autre forme juridique. Les associés y répondent solidairement et de manière illimitée. C'est la qualification par défaut d'une *DAO* sans enveloppe juridique.

Single-currency stablecoin (SCS) — Catégorie réglementaire de la MAS (« stablecoin à monnaie unique »), annoncée le 15 août 2023, visant un stablecoin arrimé au dollar de Singapour ou à une monnaie du G10 et émis à Singapour dans le respect d'exigences en matière de réserves, de fonds propres, de remboursement et d'information. Seuls les émetteurs conformes peuvent utiliser la mention « MAS-regulated stablecoin ».

Slashing — Destruction d'une partie des jetons mis en jeu par un *validateur*, à titre de sanction pour manquement ou indisponibilité dans le cadre de la *preuve d'enjeu*. C'est un risque que les dépositaires proposant du *staking* doivent communiquer et gérer.

Smart contract — Programme stocké sur un registre qui s'exécute lorsqu'une transaction l'appelle. C'est un outil d'exécution, et non en soi un contrat au sens juridique. L'existence d'un contrat juridique entre les parties qui interagissent avec lui relève du droit ordinaire des contrats.

© 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.

Soulbound token — *NFT* non transférable lié à une adresse et utilisé comme justificatif ou attestation. Il échappe à toute typologie financière, puisqu'il ne peut être ni négocié ni utilisé comme moyen de paiement.

Stablecoin — Jeton conçu pour conserver une valeur constante par rapport à une référence, généralement une monnaie fiduciaire. Le chapitre IV le classe, selon la promesse de remboursement qui le sous-tend, en stablecoin adossé à une monnaie fiduciaire, adossé à des crypto-actifs ou algorithmique.

Staking — Engagement de jetons dans un réseau à *preuve d'enjeu* afin de percevoir des récompenses de validation, selon des modèles allant du staking individuel au *staking délégué*, au staking en dépôt et au *liquid staking*. La communication FINMA sur la surveillance 08/2023 du 20 décembre 2023 fixe les conditions suisses du staking en dépôt.

Jeton (token) — Unité de valeur ou de droit inscrite sur un registre distribué. Cet ouvrage emploie ce terme pour toute unité de ce type et réserve « crypto-actif » et « actif numérique » à la catégorie générale.

Valeur totale bloquée (total value locked, TVL) — Valeur agrégée des actifs déposés dans un protocole DeFi ou dans l'ensemble du secteur. Elle mesure la taille, mais ne dit rien de la sécurité.

Travel rule — Exigence du GAFI, mise en œuvre en Suisse par l'art. 10 OBA-FINMA et à Singapour par la MAS Notice PSN02, selon laquelle des informations sur le donneur d'ordre et le bénéficiaire doivent accompagner les transferts de crypto-actifs entre intermédiaires réglementés.

Portefeuille non hébergé (unhosted wallet) — *Portefeuille* contrôlé par son utilisateur et non par un intermédiaire réglementé, également appelé portefeuille auto-hébergé ou privé. Les transferts depuis et vers des portefeuilles non hébergés sont soumis, dans les deux places, à des exigences spécifiques en matière de travel rule et de diligence.

© 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.

Jeton d'utilité (utility token) — Catégorie de la FINMA désignant un jeton qui donne un accès numérique à une application ou à un service. Il échappe au droit des valeurs mobilières si le service existe au moment de la vente. La FINMA le traite comme un *jeton d'investissement* s'il est vendu pour financer un service qui n'est pas encore opérationnel.

Modèle UTXO (UTXO model) — Architecture de registre, utilisée par Bitcoin, dans laquelle la valeur est suivie sous forme de sorties de transaction non dépensées distinctes, chacune dépensée en totalité et remplacée par de nouvelles sorties. Contrairement au *modèle à comptes*, il permet un traçage fondé sur la filiation.

Validateur (validator) — Participant à un réseau à *preuve d'enjeu* qui propose et atteste des blocs après avoir bloqué des jetons à titre de caution. Il perçoit des récompenses pour une participation honnête et s'expose au *slashing* en cas de manquement.

Portefeuille (wallet) — Logiciel ou matériel qui conserve des *clés privées* et signe des transactions. Il ne contient rien d'autre que des clés, car les jetons eux-mêmes restent sur le registre.

Livre blanc (white paper) — Document décrivant un projet de jeton, sa technologie et son modèle économique. Sous MiCA, c'est un document d'information réglementé. Sous la LSFin et le SFA, il peut constituer un prospectus si le jeton est une valeur mobilière et qu'aucune exemption ne s'applique.

Jeton enveloppé (wrapped token) — Jeton sur un registre représentant un jeton bloqué sur un autre au moyen d'un *pont*, dont WBTC est l'exemple principal. Économiquement, il s'agit d'une créance contre la personne qui contrôle l'actif bloqué.

Preuve à divulgation nulle de connaissance (zero-knowledge proof) — Méthode cryptographique par laquelle une partie prouve qu'une affirmation est vraie sans révéler les données sous-jacentes. Elle est utilisée dans les *rollups* à des fins d'évolutivité et dans les systèmes d'identité pour prouver des attributs, tels que l'âge

© 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.

ou la juridiction, sans divulguer l'identité. Les parties F et L examinent son intérêt pour la conception des dispositifs de conformité en matière de lutte contre le blanchiment.

Notes

1. Loi sur le blanchiment d'argent, RS 955.0, art. 2, al. 3 (intermédiaires financiers du secteur non bancaire). Partie F, chapitre I. ↩
2. Payment Services Act 2019 (Singapour), section 2(1). La définition exclut la *monnaie électronique* et les *DPT à usage limité*. Partie K, chapitre I. ↩
3. Code des obligations, RS 220, art. 973d–973i. Partie D, chapitre 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. 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