2026

FRANCE PAYMENTS FORUM

GLOSSAIRE DES CRYPTOPAIEMENTS

Avant-propos

Depuis la première édition du Glossaire des Cryptopaiements publié par France Payments Forum en novembre 2020, le paysage des paiements numériques a connu des transformations d'une ampleur que peu auraient anticipée. Ce qui relevait alors d'un domaine encore confidentiel, bien souvent porté par des pionniers des cryptoactifs, est devenu en quelques années un sujet de premier plan, au croisement des agendas réglementaires, géopolitique, monétaires et industriels à l'échelle mondiale.

Dix-sept ans après l'invention du Bitcoin, et avec l'essor des blockchains alternatives et de leurs écosystèmes, l'industrie des paiements a progressivement intégré ces technologies dans des cas d'usage couvrant l'ensemble de la chaîne de valeur : émission et conservation de cryptoactifs, moyens de paiement décentralisés, stablecoins adossés à des actifs traditionnels, finance décentralisée (DeFi), etc... Cette dynamique ne marque pas seulement une évolution technologique, elle interroge en profondeur les fondements mêmes de notre système monétaire et financier.

Ce mouvement a pris en Europe une dimension particulière. L'adoption du règlement MiCA constitue une première mondiale : un socle commun pour l'ensemble du marché européen. Mais au-delà de la réglementation, c'est toute une dynamique industrielle qui s'organise. Des consortiums se constituent regroupant banques, fintechs, infrastructures de marché et acteurs du paiement, pour construire ensemble les rails de la prochaine génération de paiements. Ces initiatives collectives témoignent d'une prise de conscience : la transformation en cours ne peut être menée isolément. Elle exige une coopération à une échelle inédite, où les frontières traditionnelles entre secteurs public et privé, entre acteurs nationaux et européens, s'estompent au profit de projets communs.

Ce qui frappe, rétrospectivement, c'est la vitesse à laquelle certaines technologies sont passées du stade de la promesse à celui du standard. La tokénisation des actifs, les paiements transfrontaliers, l'interopérabilité entre blockchains : autant de sujets qui, il y a cinq ans encore, relevaient de la promesse théorique, et qui font aujourd'hui l'objet de déploiements réels. Ce basculement est important à noter, car il change la nature même du débat : il ne s'agit plus de savoir si ces technologies vont s'imposer, mais comment les encadrer, les déployer et les rendre accessibles au plus grand nombre.

Dans ce contexte, la clarté du langage n'est pas un luxe. Elle est une condition de base pour que les décideurs, les régulateurs, les professionnels du secteur et, plus largement, le grand public puissent participer à des débats qui les concernent directement. Car ce sont bien des choix de société qui se jouent : quelle souveraineté monétaire pour demain ? Quelle place pour les acteurs privés face aux institutions publiques ? Quelle protection pour les utilisateurs dans des environnements encore largement en construction ?

C'est dans cet esprit que le GT Cryptopaiements de France Payments Forum a élaboré et fait évoluer ce glossaire. Il ne s'agit pas simplement de compiler des définitions techniques. Il s'agit de poser un cadre commun, accessible et rigoureux, qui permette à chacun de s'approprier un vocabulaire en pleine mutation. Ce travail collectif, porté par des professionnels engagés, reflète la conviction que l'éducation et la compréhension partagée sont des préalables indispensables à toute régulation intelligente et à toute adoption responsable.

Cette nouvelle édition tient compte des évolutions intervenues depuis la première version : l'adoption du règlement européen MiCA, les avancées des projets de MNBC, l'émergence de nouveaux modèles comme la tokénisation des actifs du monde réel (RWA), ou encore la maturation progressive des infrastructures de paiement on-chain. Le vocabulaire s'est enrichi, précisé, parfois stabilisé, mais il reste vivant, et ce glossaire avec lui.

Glossaire

A

2 Aave

Protocole de finance décentralisée (DeFi) permettant de prêter et d'emprunter des cryptoactifs sans intermédiaire centralisé. Les utilisateurs peuvent déposer des actifs dans **des pools de liquidité** et recevoir en contrepartie des jetons **représentatifs de leur dépôt** (aTokens), qui génèrent des intérêts. D'autres utilisateurs peuvent **emprunter ces actifs** contre dépôt de collatéral, avec des taux variables ou stables, et des mécanismes de liquidation en cas d'insuffisance de garanties. Aave fonctionne principalement sur Ethereum et d'autres blockchains compatibles EVM, et constitue l'un des protocoles DeFi les plus importants en termes de Total Value Locked (TVL).

3 ABI

Application Binary Interface (ABI), format décrivant comment interagir avec un **smart contract** (fonctions, types, événements).

4 Actif
Asset

Ressource ou élément de valeur qu'un individu ou une organisation peut détenir ou contrôler, et dont l'usage, la détention ou le transfert peut produire un bénéfice, un droit, un revenu ou un avantage. Exemples : liquidités, créances, actions, biens immobiliers, droits d'usage, données, licences, jetons numériques.

5 Actif fungible
Fungible Token

Un **actif** est dit **fongible** lorsqu'il peut être remplacé par un autre **actif** de même nature à valeur équivalente, les unités étant interchangeables. Exemples : l'euro ; les unités de bitcoin ou d'ether ; les jetons ERC-20. Voir aussi : **Fongibilité**.

6	**Actif Non Fongible** *Non-Fungible Token (NFT)*	Les **actifs** non **fongibles** possèdent des caractéristiques intrinsèques qui les rendent uniques et non interchangeables. Exemple : Timbre à collectionner, maison, toile de maître, etc. Le standard NFT **ERC721** de la blockchain Ethereum permet de représenter sous forme de token le droit de propriété exclusif sur un objet numérique (œuvre d'art digitale, carte à collectionner numérique, etc) et s'apparente ainsi à un certificat d'authenticité. Le marché des NFT a explosé en 2021 et propulsé par la même occasion la start-up blockchain Sorare à la deuxième place des licornes françaises en terme de valorisation.
7	**Actif numérique** *Digital Asset*	Un **actif numérique** (ou **virtuel**) peut recouvrir, selon les usages, un actif dématérialisé (années 90), un actif électronique (années 2000) ou un actif numérique au sens "crypto" (années 2020). Un actif dématérialisé est un actif conçu à l'origine sous une forme matérielle (métal, papier, autre matière, etc.) pour être stockable et échangeable manuellement, puis transposé en donnée électronique nouvelle (par exemple via numérisation pour certains actifs papier). Un actif électronique est un actif conçu dès l'origine sous forme électronique, afin d'être stockable et échangeable directement sous cette forme. Un actif numérique est un actif électronique dont l'émission et le transfert sont généralement organisés au moyen de mécanismes cryptographiques et, le plus souvent, via une technologie de registre distribué (**DLT**). Les termes actif numérique et **cryptoactif** sont souvent confondus dans l'usage.Référence réglementaire en droit français voir l'article L.54-10-1 du Code monétaire et financier.
8	**ADA**	**Cryptomonnaie** native de la **blockchain Cardano** ; utilisé notamment pour payer les frais de transaction, participer au mécanisme de validation (**staking**) et interagir avec les applications de l'écosystème **Cardano**. Voir **Cardano**.
9	**Adresse** *Adress*	Une adresse est une suite de caractères alphanumériques représentant l'identité de l'utilisateur sur le réseau **blockchain**. Elle dérive généralement de la **clé publique** sur laquelle est appliquée une ou plusieurs fonctions de hachage. On peut comparer une adresse à un IBAN.
10	**Algorithme de consensus** *Consensus Algorithm*	Mécanisme par lequel les **nœuds valideurs** d'un **registre distribué** entérinent un nouveau bloc d'opérations.
11	**Altcoin**	**Cryptoactif** alternatif au **bitcoin**
12	**AML**	AML – Anti-Money Laundering. *Voir* **LCB-FT**
13	**AMM**	Un **Automated Market Maker** (AMM) est un protocole d'échange décentralisé. Il permet d'échanger des **actifs numériques** de manière automatique et sans autorisation en utilisant des **pools de liquidités** plutôt qu'un marché traditionnel à carnet d'ordres avec des acheteurs et des vendeurs. Les AMM sont basés sur des formules mathématiques, permettant d'estimer le taux de change entre deux **actifs**, en prenant en compte les liquidités apportées par les utilisateurs. La formule mathématique est généralement une fonction constante de type x*y=k qui établie le prix pour une paire de tokens en fonction des liquidités disponibles. Ainsi, lorsque la quantité du jetons x augmente, celle de y doit diminuer dans le but de garder la valeur de k constante.

14	**ART**	**Asset-Referenced Token** : Jeton référencé à un **actif.** Catégorie de **cryptoactifs** définie par **MiCA**, visant à maintenir une valeur stable en se référant à un panier d'actifs, pouvant inclure des **monnaies**, des matières premières, des **cryptoactifs** ou une combinaison de ces actifs. Un ART n'est pas limité à une seule devise : sa stabilité dépend de la qualité de son collatéral et des mécanismes de gestion associés. Les émetteurs d'ART doivent répondre à des obligations renforcées en matière de transparence, de gouvernance, de réserves et de **LCB-FT**, particulièrement lorsque les jetons sont jugés « significatifs ».
15	**Atomic Swap**	Technique d'échange décentralisé entre deux **actifs numériques** (souvent sur deux **blockchains** ou protocoles différents) reposant sur le principe d'**atomicité** : l'échange est soit exécuté intégralement pour les deux parties, soit entièrement annulé. Un atomic swap s'appuie généralement sur des **Hash TimeLock Contracts** (**HTLC**), qui imposent des conditions cryptographiques et des délais d'expiration pour garantir que les fonds ne peuvent être transférés que si les deux transactions correspondantes sont réalisées. Ce mécanisme réduit le risque qu'une partie paie sans recevoir l'actif en retour.
16	**Atomicité**	En **paiement** et en informatique, une opération est dite atomique lorsque la suite d'étapes qui la compose est indivisible : elle s'exécute entièrement, ou bien elle est entièrement annulée en cas d'échec, quel que soit le nombre d'étapes déjà réalisées. L'atomicité permet d'éviter les situations où une transaction serait partiellement exécutée (**paiement** effectué sans livraison, ou inversement). Voir aussi : **Atomic Swap**, **DvP**, **PvP**.
17	**Attaque des 51%**	Désigne une attaque dans laquelle un attaquant prend le contrôle de 51% de la puissance de **hachage** d'une **blockchain**. Il possède ainsi la majorité des votes des mineurs et peut arranger la **blockchain** en générant des risques de **double dépense** et de **censure**.
18	**Automated Market Maker**	Voir **AMM**
19	**Avalanche**	Plate-forme de **blockchain publique** de couche 1 conçue pour offrir un haut débit (jusqu'à plusieurs milliers de transactions par seconde), une finalité rapide, et une architecture modulaire à trois chaînes interopérables (X-Chain, C-Chain, P-Chain). Avalanche permet la création de réseaux souverains (« subnets ») personnalisables, tout en restant compatible avec l'**EVM** (Ethereum Virtual Machine) via sa C-Chain. Le jeton natif **AVAX** est utilisé pour payer les frais de transaction, participer à la gouvernance, **staker** pour la sécurité du réseau (**Proof of Stake**) et lancer des sous-réseaux. Caractéristiques principales : Inventeurs : Emin Gün Sirer, Kevin Sekniqi et Maofan "Ted" Yin (via Ava Labs) ; Lancement : 2020 (réseau principal) ; Monnaie interne : **AVAX**. **Turing-complet** : oui (via compatibilité **EVM** et **smart contracts** sur C-Chain). Langages principaux : **Solidity** (via **EVM**), Rust/C++/Go/etc. pour développement infrastructure. Rang / capitalisation : figure parmi les top **blockchain publiques** par capitalisation en 2025.

20	**Avalanche consensus**	Famille de protocoles reposant sur un échantillonnage aléatoire et itératif pour atteindre le consensus.
21	**AVAX**	Voir **Avalanche**

B

22	**Baker**	De l'anglais, sur le protocole blockchain Tezos, les **bakers** correspondent aux valideurs du réseau en charge de vérifier les transactions et ajouter des blocs à la chaine. La détention d'un montant minimal de tez (XTZ) est requise par le protocole pour devenir baker, conformément à l'algorithme de consensus Proof-of-Stake implémenté par Tezos.
24	**BCE** *ECB*	Banque Centrale Européenne / European Central Bank (ECB) Institution centrale de **l'Eurosystème** responsable de la politique monétaire, de l'émission de la **monnaie de banque centrale (CeBM)**, de la supervision des systèmes de paiement et de la gouvernance de **TARGET Services**. La BCE coordonne les décisions stratégiques, réglementaires et opérationnelles liées aux infrastructures de marché et aux projets tels que l'euro numérique.
25	**BCN** *NCB*	Banque centrale nationale (National Central Bank)
26	**Beacon Chain**	Chaîne de coordination d'**Ethereum PoS** gérant les **validateurs** et le **consensus**.
27	**Besu**	Hyperledger Besu: Client **Ethereum** open-source, compatible avec la machine virtuelle Ethereum (**EVM**), pouvant fonctionner en mode public (Ethereum) ou permissionné (réseaux privés). Besu supporte différents **algorithmes de consensus** comme **IBFT** et **QBFT**, ce qui le rend adapté aux cas d'usage institutionnels nécessitant contrôle, auditabilité et gouvernance. Il fournit également des outils avancés pour la gestion des nœuds, les transactions et l'observabilité du registre distribué.

28	**BFT**	De l'anglais, Byzantine Fault Tolerance : Tolérance aux fautes byzantines (BFT) Propriété d'une **technologie de registre distribué** lui permettant de continuer à fonctionner correctement même si certains **nœuds** se comportent de façon erronée ou malveillante. Un protocole BFT vise à atteindre un **consensus** malgré la présence de messages incohérents ou de participants qui ne respectent pas les règles. Ce principe est essentiel pour les réseaux utilisant un **registre distribué**, en particulier lorsque la confiance entre les **nœuds** n'est pas garantie. La BFT de Bitcoin est de 49% (Voir **Attaque des 51%**)
29	**Bitcoin**	De l'anglais coin (monnaie) et bit (unité), le terme bitcoin désigne à la fois un système de transfert d'un **cryptoactif** (on l'écrit alors avec une majuscule et sans article) et une unité de compte (on l'écrit alors sans majuscule et il peut prendre la marque du pluriel). Bitcoin (avec majuscule) est un système de transfert d'un **cryptoactif**, le bitcoin (avec une minuscule), reposant sur une **blockchain publique**.
30	**Bloc** *Block*	Un bloc est une structure de données qui contient un ensemble de transactions. Les blocs sont reliés entre eux par des outils cryptographiques pour assurer l'intégrité et la chronologie ce qui forme une **chaîne de bloc** de données (**blockchain**).
31	**Block header**	Partie d'un bloc contenant les métadonnées essentielles : horodatage, racine **Merkle**, **hachage** du **bloc** précédent, etc.
32	**Blockchain**	Une chaîne de blocs (ou blockchain), est une des formes de la **technologie de registre distribué** qui permet le stockage et l'échange de **cryptoactifs** par un système distribué sans un tiers de confiance central.
33	**Blocktime**	Durée moyenne séparant l'ajout de deux **blocs** successifs dans une **blockchain**. Le temps de bloc est un paramètre de protocole (par exemple ~10 minutes pour **Bitcoin**, ~12 secondes pour **Ethereum**) : dans un système **Proof of Work** (**PoW**), il est maintenu en ajustant la **difficulté** de **minage** afin que la recherche du **nonce** prenne en moyenne ce délai, compte tenu de la puissance de calcul disponible ; dans les systèmes basés sur la **preuve d'enjeu** (**PoS**), il est généralement déterminé par la durée des slots ou des epochs définis par le protocole. Le temps de bloc influence directement la latence de confirmation des transactions et la perception de leur finalité.
34	**BNB**	De l'anglais, Build N Build Chain, Écosystème de **blockchains** lancé par Binance, comprenant : Écosystème de **blockchains** initialement lancé par Binance, comprenant : la BNB Smart Chain (BSC) (ex Binance Smart Chain) : **blockchain** compatible **EVM** orientée **smart contracts**, rapide et à faible coût ; la BNB Beacon Chain (ex Binance Chain) : couche de gouvernance et de staking. La **monnaie** interne BNB (anciennement Binance Coin, désormais interprété comme Build N Build) sert au paiement des frais, à la gouvernance ainsi qu'à la validation via la preuve d'enjeu déléguée (**dPoS**). BNB Chain héberge un vaste écosystème **DeFi**, **DEX**, **NFT**, jeux et protocoles multi-chaînes.

35 **Burn**

Procédure consistant à détruire définitivement des jetons en les retirant de la circulation (par exemple en les envoyant vers une adresse irrécupérable). Le burn réduit l'offre totale et s'effectue souvent lors du **defund**, ou dans des modèles économiques déflationnistes.

36 **Bytecode**

Code compilé exécuté par la machine virtuelle Ethereum (**EVM**).

C

37 **Canaux de paiement**
Payment Channel

Au sein de la technologie de registre distribué, c'est un mécanisme permettant d'effectuer plusieurs transactions hors chaîne entre deux parties, avec règlement final sur la blockchain, afin d'améliorer la rapidité et de réduire les coûts. Exemple : Lightning Network (Bitcoin). Cette terminologie est utilisée dans plusieurs écosystèmes blockchain ; à ne pas confondre avec les « channels » d'Hyperledger Fabric, qui désignent plutôt un sous-réseau privé de communication entre organisations pour isoler les échanges et la visibilité des transactions.

38	**Cardano (ADA)**	Plateforme de **blockchain publique** fondée sur un mécanisme de **Proof of Stake** (Ouroboros), avec un fort accent sur la recherche académique et la vérification formelle. Cardano supporte des **smart contracts** (modèle eUTxO) et héberge un écosystème croissant de **dApps**, notamment dans la **DeFi**, avec un positionnement orienté "sécurité / formalisation". Caractéristiques principales : Inventeur : Charles Hoskinson (cofondateur d'Ethereum, fondateur d'IOHK / Input Output). Lancement : réseau principal Cardano (Byron) en 2017 ; **smart contracts** (Alonzo) disponibles depuis 2021. Monnaie interne : ADA. **Turing-complet** : oui, via les langages de **smart contracts** sur la couche de calcul (Plutus). Langages principaux : Plutus (basé sur Haskell), Marlowe (DSL pour contrats financiers). Rang / market cap (2025) : reste dans le top 10 des **cryptoactifs** par capitalisation, malgré une forte volatilité
39	**Cash**	*Voir* **Monnaie fiduciaire**
40	**CASP**	Crypto-Asset Service Provider. Voir **PSCA**
41	**CeBM**	Central Bank Money, voir **Monnaie de banque centrale**
42	**Censure** *Censorship*	Action de contrôler, restreindre ou empêcher la diffusion, l'accès ou l'exécution de certaines informations, contenus ou opérations, généralement via des règles de filtrage. Dans les **paiements**, capacité d'un intermédiaire (banque, **PSP**, acquéreur, réseau, processeur) à refuser, bloquer, retarder ou annuler une opération, ou à restreindre l'accès au service, sur la base de règles de conformité (AML/CFT, sanctions), de gestion du risque (fraude, chargebacks), de politiques commerciales (secteurs interdits), ou d'injonctions d'autorités. Peut viser un payeur, un bénéficiaire, un marchand, un pays, un type d'opération ou un usage.
43	**CFT**	Tolérance aux fautes classiques (CFT). De l'anglais, Crash Fault Tolerance, propriété d'un système distribué dans lequel les **nœuds** peuvent tomber en panne ou cesser de répondre, mais ne sont pas malveillants. Un protocole CFT permet d'atteindre un **consensus** tant que les pannes concernent uniquement des **nœuds** inactifs mais honnêtes. Ce modèle est plus simple que le **BFT**, mais ne protège pas contre les comportements adverses.
44	**Chaincode**	Dans **Hyperledger Fabric**, unité de code déployée sur le réseau qui exécute la logique métier des transactions (règles de lecture/écriture de l'état du registre). Il correspond fonctionnellement à un **smart contract**, avec une nuance pratique : le chaincode est l'unité technique de déploiement pouvant embarquer une ou plusieurs logiques de "contrat" selon l'organisation du code.
45	**Chaîne de blocs**	Voir **blockchain**
46	**Chaîne de blocs latérale ou adjacente** *Sidechain*	Une chaîne de blocs latérale ou sidechain est une méthode de séparation des **blockchains** en deux groupes, un primaire, et un secondaire, ce qui permet à un utilisateur de transférer ses **actifs numériques** dans un premier groupe avec des

services spécifiques et séparés mais reliés au deuxième pour des services supplémentaires.

47	**Chaîne de blocs permissionnée** *Permissioned blockchain*	Caractéristique d'une **chaîne de blocs privée** dont la participation et l'accès sont réglementés et réservés aux seuls participants autorisés.
48	**Chaîne de blocs privée** *Private blockchain*	**Blockchain** dans laquelle tous les nœuds appartiennent à une entité ou à un groupe d'entités (consortium) qui contrôle accès, écriture et consensus.
49	**Chaîne de blocs publique** *Public blockchain*	**Blockchain** totalement distribuée, à laquelle l'accès aux participants n'est pas règlementé (permissionless) pour devenir un **nœud valideur** et dans laquelle tous les nœuds possèdent le même rôle sans aucun nœud dominant (pair à pair).
50	**Clé privée** *Private Key*	Une clé privée, connue du seul propriétaire du **wallet**, permet de signer des transactions et prouver à l'ensemble des participants du réseau que l'on est le propriétaire d'une adresse à laquelle est associé un solde de **cryptoactifs**. On peut comparer la clé privée au code secret permettant d'accéder à sa banque *Voir* **Cryptographie asymétrique**
51	**Clé publique** *Public Key*	La clé publique, connue de tous, permet à quiconque, et en particulier aux **validateurs** du réseau, de vérifier la signature d'une transaction produite par la **clé privée** correspondante. Elle est générée à partir de la **clé privée** à l'aide d'une fonction **cryptographique** irréversible. *Voir* **Cryptographie asymétrique**
52	**CLM**	Central Liquidity Management Module central de **TARGET Services** permettant la gestion consolidée de la liquidité des participants dans **l'Eurosystème**. CLM regroupe les **MCA**, offre une vue agrégée de la trésorerie disponible, et permet de répartir la liquidité vers les différents modules (**RTGS**, T2S, TIPS). CLM fournit les services de gestion de liquidité, d'ordonnancement, de files d'attente et de contrôle des positions.
53	**CoBM**	Commercial Bank Money **Monnaie** émise par les banques commerciales, principalement sous forme de dépôts sur comptes (**monnaie scripturale**). Elle est créée notamment lorsque les banques accordent des crédits, ce qui génère un dépôt au nom de l'emprunteur. Voir également **Monnaie de banque centrale** et **CeBM.**
54	**Collateralized token**	Jeton dont la valeur est garantie par un collatéral détenu en réserve.
55	**Compound**	Protocole de prêt/emprunt décentralisé permettant aux utilisateurs de déposer des **cryptoactifs** dans des pools pour générer des intérêts, ou d'emprunter contre dépôt de collatéral. Les déposants reçoivent des cTokens, qui représentent leur position et accumulent les intérêts. Compound est un des protocoles **DeFi** les plus anciens et a fortement influencé les modèles de lending automatisé.

56	**Consensus**	Voir **Algorithme de consensus.**
57	**Contrat intelligent** *Smart Contract*	Contrat intelligent, ou programmable ou auto-exécutant, il s'agit d'un programme informatique autonome qui s'appuie sur la **technologie de registre distribué** (**DLT**) pour exécuter les termes d'un contrat, sans avoir nécessairement recours à une autorité centrale pour être déclenché.
58	**Convertibilité**	La convertibilité est la capacité légale à échanger une **monnaie** contre une autre devise, mais sans garantie de valeur
59	**Corda**	Plateforme de **technologie de registre distribué DLT** "permissionnée" développée par R3 en 2014, conçue pour des cas d'usage institutionnels (notamment finance/paiements) où les participants sont identifiés et où la confidentialité est essentielle. Contrairement aux **blockchains** à diffusion globale, Corda fonctionne principalement en pair-à-pair : seules les parties concernées reçoivent les données d'une opération ("need-to-know"). La validation repose sur (i) la validité (règles/contrats) et (ii) l'unicité (prévention du double-emploi) assurée par un service de notaire.
60	**Cosmos SDK**	Cadre de développement permettant de créer des blockchains personnalisées interopérables via IBC.
61	**Cours legal** *Legal Tender*	Étymologiquement, « Ayant cours légal » signifie pouvant circuler « de par la loi ». Le cours légal est un privilège accordé par la loi à un **moyen de paiement**. Il s'applique aujourd'hui uniquement à la **monnaie fiduciaire** (pièces et billets). Il recouvre quatre notions : (1) le pouvoir libératoire; (2) l'acceptation à la valeur nominale; (3) l'acceptation obligatoire par le créancier, (4) le cours forcé (qui renvoie outre à la circulation exclusive de la monnaie, à sa valeur et aux modalités de sa fixation). La première notion est commune à toutes les acceptions. Toutefois, la portée juridique du cours légal peut varier d'un pays à l'autre (y compris en Europe). Ainsi par exemple en droit européen, cette notion concerne les billets et les pièces en euro, et recouvre leur pouvoir libératoire, mais peut avoir d'autres attributs selon les pays. En droit français, cela recouvre l'acceptation obligatoire en paiement ; le fait de refuser un paiement en billets ou en pièces ayant cours légal en France est puni d'une amende. Au Royaume-Uni, le cours légal est restreint au pouvoir libératoire et n'inclut pas l'acceptation obligatoire. Par ailleurs le cours légal peut être limité par des plafonds (en France le plafond est fixé à 1000 euros)
62	**Crash Fault Tolerance**	Voir **CFT**
63	**Cross-chain bridge**	Mécanisme permettant de transférer des **actifs** entre différentes blockchains.
64	**Cryptanalyse** *Cryptanalysis*	Technique qui consiste à déduire un texte en clair à partir d'un texte crypté sans posséder la clé de décryptage.
65	**Crypto-jeton** *Crypto-token, Digital Token*	Jeton numérique cryptographique géré par la technologie de registre distribué
66	**Cryptoactif** *Cryptoasset*	Un cryptoactif est une forme de bien ou patrimoine immatériel dont le principal de sa structure ou composition est porté par la **technologie de** registre distribué
67	**Cryptoactif stable** *Stablecoin*	**Cryptoactif** visant à maintenir la parité avec un autre **actif** de référence, le plus souvent une **monnaie légale** ou des métaux précieux (or, argent, etc. quelle que soit leur forme : barre, pièces, ou autre)

68	**Cryptoactif stable algoritmique** *Algorithmic stablecoin*	**Cryptoactif stable** doté d'un mécanisme automatique de stabilisation de sa valeur par rapport à son **actif** de référence.
69	**Cryptoactif stable adossé à des actifs financiers** *Asset-linked Stablecoins*	**Cryptoactif stable**, s'appuyant sur un panier d'actifs financiers. La stabilité du stablecoin repose sur des opérations de vente du **cryptoactif** lorsqu'il est au-dessus de sa valeur de parité et d'achat lorsqu'il est en-dessous.
70	**Cryptographie** *Cryptography*	La cryptographie est une des disciplines de la **cryptologie** s'attachant à protéger des messages assurant les 5 fonctions : identification, authentification, intégrité, confidentialité et non-répudiation.
71	**Cryptographie asymétrique** *Asymmetric cryptography*	Technique **cryptographique** qui sert à sécuriser l'information et les systèmes grâce à un algorithme utilisant deux clés : une **clé privée** (non partagée) pour signer un message en clair ou décrypter un message reçu, et une clé publique (partagée avec les personnes autorisées) pour authentifier un message reçu ou crypter un message clair à envoyer.
72	**Cryptographie symétrique** *Symmetric cryptography*	Technique **cryptographique** rapide qui utilise une clé unique et secrète pour le cryptage et le décryptage.
73	**Cryptologie** *Cryptology*	Étymologiquement, science du secret, la cryptologie est la science et branche des mathématiques qui concerne la sécurité de l'information. Elle englobe la **cryptographie** et la **cryptanalyse**.
74	**Cryptomonnaie** *Cryptocurrency*	Étymologiquement, une cryptomonnaie est une **monnaie** basée sur un système **cryptographique** plutôt que sur la confiance en un tiers (comme une banque centrale) pour effectuer des transactions. Un **cryptoactif** qui possède les propriétés de la monnaie peut être appelé **cryptomonnaie**.
75	**Cryptopaiement** *Cryptopayment*	**Paiement** réalisé avec une **monnaie numérique** commerciale ou de banque centrale, ou par cession d'un **cryptoactif**, ou par une **monnaie scripturale**, via un **moyen de paiement** utilisant la **technologie de registre distribué**.
76	**Curve**	Curve Finance. Protocole **DeFi** spécialisé dans les échanges entre **stablecoins** et **actifs** ayant une valeur proche (stables ou **staked**), utilisant un **AMM** optimisé pour réduire le slippage et les pertes impermanentes. Curve est structuré autour de **pools de liquidité** particulièrement adaptés aux **stablecoins** (**DAI**, **USDC**, **USDT**, etc.) et constitue un pilier stratégique de la liquidité stable dans la **DeFi**.

D

77	**DAI**	Stablecoin décentralisé émis par le protocole MakerDAO et visant à maintenir une parité de 1 DAI = 1 USD. Contrairement aux stablecoins centralisés (comme USDT ou USDC), DAI est créé lorsque des utilisateurs déposent des collatéraux (par exemple ETH, WBTC, ou même des stablecoins) dans des coffres (vaults) du protocole. Le montant de DAI émis dépend du ratio de collatéralisation, qui doit rester supérieur à un seuil déterminé pour éviter la liquidation. La stabilité du peg est maintenue via des mécanismes économiques programmés (taux d'épargne DAI – DAI Savings Rate, frais de stabilité, arbitrages, gestion du surplus). DAI est un stablecoin clé de la DeFi, largement utilisé dans les plateformes de lending, AMM, farming et paiements.
78	**DAO**	De l'anglais Decentralized Autonomous Organization. Organisation gouvernée par des règles automatisées codées dans des **smart contracts**.
79	**Dapps** *Distributed Application*	Acronyme anglais qui signifie « application distribuée » ou parfois décentralisée. Il s'agit d'un logiciel utilisant des **contrats intelligents** (**smart contracts**) et qui opère d'une façon autonome grâce à la technologie de registre distribué.
80	**Dark Pool**	Désigne des places de marchés où les échanges se font de gré à gré (OTC). C'est un moyen souvent utilisé par les institutionnels afin de ne pas influencer le marché. (similaire aux dark pools des marchés actions.)
81	**DCA**	Dedicated Cash Account. Compte en monnaie banque centrale ouvert dans **TARGET Services** (T2/TIPS), utilisé pour le règlement de paiements ou **d'actifs tokenisés** dans le cadre des projets d'**euronumérique de gros** ou des **DLT** d'institutions financières. Un DCA permet d'isoler les liquidités dédiées au règlement sur une infrastructure donnée, tout en garantissant la finalité en monnaie banque centrale.
82	**DCW**	Dedicated Cash Wallet. Instrument ou "**wallet**" associé à un **Dedicated Cash Account** (**DCA**) dans les expérimentations de **l'Eurosystème** pour le règlement d'actifs tokenisés. Le DCW représente la portion du **DCA** accessible sur une **DLT**, permettant d'utiliser de la **monnaie banque centrale** tokenisée dans les mécanismes de **DvP**, **PvP**, ou dans les tests de règlement interbancaire programmables.
83	**Decentralized Exchange (DEX)**	*Voir* **DEX**

84	**DEEP** *DLT*	Dispositif d'Enregistrement Electronique Partagée (DEEP) : il s'agit de la technologie plus communément désignée sous le terme de **technologie de registre distribué** ou **Distributed Ledger Technology** (**DLT**) ou **blockchain**.
85	**DeFi**	**Finance Décentralisée** de l'anglais Decentralized Finance Concept faisant référence aux applications financières traditionnelles (comme les prêts) utilisant la **blockchain** et les **cryptoactifs**. La DeFi vise à créer un ensemble de services financiers (dépôts, emprunts, ...) opensources, décentralisés, transparents et ouverts à tous.
86	**Defund**	Action consistant à décréditer ou retirer des **actifs** d'un compte, d'un **wallet**, d'un **smart contract** ou d'un **jeton**, en ramenant les fonds vers un compte de référence. Dans le cadre de **l'Eurosystème**, le defund peut désigner le transfert sortant depuis un **DCA** (**RTGS**) ou un **MCA** (**CLM**) vers un autre compte de paiement ou de trésorerie. Dans les systèmes de **tokenisation**, le defund est souvent couplé à une opération de burn, où les **jetons** représentatifs de l'**actif** sont détruits lorsque l'**actif** sous-jacent est restitué.
87	**Délégation de vote** *Delegated Voting*	Transfert de ses droits de vote à un autre utilisateur.
88	**Depegging**	Perte, temporaire ou durable, de l'ancrage d'un **stablecoin** ou d'un **actif** indexé (par exemple sur l'euro ou l'or) lorsque son prix s'écarte significativement de la valeur de référence. Le depegging peut résulter d'un manque de liquidité, d'une perte de confiance, d'un problème de collatéral ou d'attaques de marché. Il remet en cause la fonction principale du **stablecoin**, qui est de maintenir une valeur stable par rapport à un **actif** de référence.
89	**Déploiement déterministe** *Deterministic Deployment*	Méthode garantissant que l'adresse d'un contrat est prévisible avant son déploiement (ex : CREATE2).
90	**Deposit Token**	Terme utilisé dans les discussions européennes (**MiCA** / **Euronumérique** / **tokenisation**) pour désigner un **jeton** émis par une banque commerciale, représentant une créance sur un dépôt bancaire traditionnel. Un Deposit Token est : une forme tokénisée de **monnaie scripturale**, émise par une banque réglementée, utilisable sur une infrastructure **DLT** pour des paiements, **DvP**, **PvP**, ou des cas d'usage programmables. Il ne s'agit pas d'un **EMT** ni d'un **ART** : son statut dépend du droit bancaire (monnaie de banque commerciale), et il n'est pas toujours couvert par **MiCA** mais par la réglementation bancaire. Les Deposit Tokens sont considérés comme un élément clé des architectures de paiements tokenisés et des projets de **l'Eurosystème**.
91	**Devise** *Currency*	Le terme français désigne exclusivement les **monnaies** étrangères à un pays ou une zone monétaire donnée. C'est une **monnaie** qui circule en dehors des territoires où elle est émise et où elle a « **cours légal** ».

92	**DEX** *Decentralized Exchange*	Plateforme d'échanges de **cryptoactifs** décentralisée. Les DEX utilisent souvent des **automated market makers** (**AMM**) pour apporter de la liquidité aux investisseurs impliquant l'usage de **blockchains** et les **DApps**.
93	**Difficulté**	Dans le contexte du **minage,** paramètre d'un système **Proof of Work** (**PoW**) qui ajuste le niveau de difficulté du problème cryptographique à résoudre pour produire un nouveau **bloc** afin de maintenir un **temps de bloc** moyen proche de la valeur cible définie par le protocole. Plus la difficulté de **minage** est élevée, plus il est coûteux en puissance de calcul de trouver un **nonce** donnant un hachage conforme aux règles du protocole. Dans **Bitcoin**, la difficulté est recalculée automatiquement tous les 2016 **blocs**, soit environ toutes les deux semaines, afin d'assurer un **temps de bloc** moyen autour de 10 minutes. Ce réajustement garantit que, même si le **hashrate** de calcul globale augmente ou diminue, le protocole conserve son rythme de fonctionnement prévu automatiquement.
94	**DLT**	Technologie permettant de créer et faire fonctionner par des **smart contracts** un **registre distribué** grâce à un réseau d'ordinateurs qui synchronisent, opèrent et sécurisent des **blocs** de transactions ajoutées par les **nœuds valideurs** grâce à un **mécanisme de validation**.
95	**Double dépense** *Double spending*	Acte frauduleux dans lequel le même **cryptoactif** ou jeton est dépensé plus d'une fois
96	**dPoS**	**Preuve d'enjeu** déléguée – dPoS. Delegated **Proof of Stake** Mécanisme de **preuve d'enjeu** déléguée, variante du **PoS**, dans lequel les détenteurs de **jetons** ne valident pas directement les **blocs** mais délèguent leur pouvoir de **validation** à un nombre limité de **validateurs** ou producteurs de **blocs** élus. Les validateurs sélectionnés assurent la production des **blocs** et la sécurité du réseau, tandis que les délégants reçoivent une part des récompenses. Le dPoS permet une finalité rapide, une scalabilité élevée, et une gouvernance plus active, mais repose sur un nombre réduit de validateurs, ce qui peut diminuer la décentralisation. Utilisé notamment par **BNB** Chain, EOS, Tron et certaines sidechains **PoS**.
97	**DvP**	Delivery versus Payments DvP. Mécanisme de règlement garantissant que la livraison d'un titre (transfert de propriété) n'a lieu que si le **paiement** correspondant est effectué. Dans des architectures traditionnelles, la livraison et le **paiement** peuvent être gérés par des systèmes distincts mais coordonnés. Dans certaines architectures sur **DLT** (titres tokenisés et monnaie numérique/tokenisée sur une même infrastructure), le **DvP** peut être réalisé de manière **atomique**, c'est-à-dire au sein d'une même opération : la livraison et le paiement sont exécutés ensemble, ou bien l'ensemble est annulé, ce qui élimine l'exécution partielle.

E

98	ECDSA	Algorithme de signature numérique basé sur courbes elliptiques, utilisé notamment par Bitcoin.
99	EigenLayer	Protocole permettant le restaking des validateurs Ethereum vers d'autres services.
100	EIP	Ethereum Improvement Proposal (EIP). Les EIPs sont des standards proposés par la communauté afin d'améliorer **Ethereum** : elles peuvent déboucher sur des améliorations du protocole, des APIs ou des standards de **smart contracts**. Les EIPs sont au cœur du mécanisme **off-chain** de gouvernance d'Ethereum.
101	Elliptic Curve Cryptography	**Cryptographie asymétrique** basée sur les courbes elliptiques utilisée pour les signatures et **clés publiques**.
102	EMT	Jetons de **monnaie électronique** de l'anglais Electronic Money Tokens (e-money token). Catégorie de **cryptoactifs** définie par le règlement **MiCA**, visant à maintenir une valeur stable en étant entièrement adossée à une seule **monnaie** ayant **cours légal** (ex. euro ou dollar). Un EMT fonctionne de manière proche de la **monnaie électronique**, avec obligation pour l'émetteur de détenir des **actifs** de réserve équivalents à la valeur émise. Les EMT peuvent servir de support aux **cryptopaiements**, notamment sur **blockchains publiques** ou **privées**, et constituent la forme de **stablecoin** réglementée la plus proche de la **monnaie scripturale** traditionnelle.
103	Entropie	Dans le contexte de la **blockchain**, c'est la mesure du niveau d'aléa utilisé pour générer des **clés cryptographiques** sécurisées.
104	EOA	Externally Owned Account: Compte contrôlé par une clé privée, opposé aux smart contracts qui ne possèdent pas de clé.
105	Epoch	Unité de temps regroupant plusieurs slots dans **Ethereum PoS**.
106	ERC1155	Standard de jetons multi-actifs permettant de gérer des **jetons fongibles** et **non fongibles**.
107	ERC20	Standard technique pour le développement de tokens ou **cryptoactif** sur la **blockchain Ethereum** (ERC20). Ce standard décrit les fonctions d'interface normées des **contrats intelligents** (**smart contracts**) sur le réseau distribué.
108	ERC4626	Standard définissant les coffres (vaults) de rendement pour uniformiser dépôts et retraits.
109	ERC721	Standard définissant une interface commune de jetons non fongibles (**NFT**). Chaque jeton possède un identifiant unique et des fonctions normalisées (ex. ownerOf, transferFrom, approve) permettant une interopérabilité entre applications.
110	Espèces *Cash*	*Voir* **Monnaie fiduciaire**
111	ETH	Voir **Ether** et **Ethereum**

112	**Ether**	L'Ether (**ETH**) est le **cryptoactif** intrinsèque de la **blockchain Ethereum** utilisé pour payer les frais de transaction du réseau.
113	**Ethereum**	Plateforme de **blockchain publique** permettant d'exécuter des **smart contracts** et des applications décentralisées (**dApps**) de manière programmable. Conçue pour dépasser le simple transfert de valeur de **Bitcoin**, Ethereum sert aujourd'hui de base à une grande partie de la **DeFi**, des **NFT**, de la **tokenisation** et des **stablecoins**. Inventeur : Vitalik Buterin (white paper 2014, conception dès 2013), lancement : réseau principal en 2015. Monnaie interne : Ether (ETH) **Mécanisme de consensus**: actuellement sur **PoS** (initialement sur **PoW**), et sur **sharding**. **Turing-complet** : oui, via la machine virtuelle Ethereum (**EVM**) qui exécute des **smart contracts**. Langages principaux : **Solidity**, Vyper (langages de **smart contracts EVM**). Rang / market cap (2025) : 2e cryptoactif mondial par capitalisation, première **blockchain** de **smart contracts**
114	**EURCV**	EUR CoinVertible (EURCV) : **Stablecoin** en euro (**EMT** au sens **MiCA**) émis par Société Générale–FORGE. EURCV est indexé 1:1 sur l'euro, adossé à des réserves en espèces, et vise des usages institutionnels (règlement, **DeFi**, **tokenisation**, paiements transfrontaliers) avec un haut niveau de conformité réglementaire. Caractéristiques principales : Devise de référence : EUR (peg 1:1). Émetteur : Société Générale–FORGE (SG-Forge). Lancement : 2023, initialement sur **Ethereum** pour clients institutionnels. Type : Electronic Money Token (**EMT**) conforme **MiCA**, totalement collatéralisé en euros. **Blockchains** : disponible sur **Ethereum**, étendu à **Solana** et **XRPL** (multichain). Rang / market cap (2024–2025) : **stablecoin** euro encore modeste (capitalisation de quelques dizaines de millions d'euros, mais en croissance)
115	**Euro numérique** *Digital Euro*	Projet de **monnaie numérique de banque centrale** (**MNBC**) porté par **l'Eurosystème**, visant à mettre à disposition du public une forme numérique de l'euro, émise par la **BCE** et les **BCN**. L'euronumérique serait un instrument de paiement en monnaie de banque centrale, utilisable pour les paiements du quotidien, en complément de la **monnaie fiduciaire** (espèces) et de la **monnaie scripturale**, et distribué via les intermédiaires (banques, PSP). Il ne s'agit pas d'une **cryptomonnaie** privée mais d'une créance directe sur la banque centrale, avec un cadre strict de protection des données, de plafonds d'avoirs et d'interopérabilité avec les systèmes de paiement existants (**TARGET Services**, schémas cartes, instant payments…).
116	**Eurosystème**	Ensemble constitué de la Banque centrale européenne (BCE) et des banques centrales nationales (BCN) des États membres de la zone euro. L'Eurosystème définit et met en œuvre la politique monétaire, gère les systèmes de règlement comme TARGET Services, supervise le fonctionnement des infrastructures de paiement et assure la stabilité de l'euro.

117	**EVM**	**Ethereum** Virtual Machine EVM. L'EVM est le composant le plus important d'**Ethereum**. Il s'agit d'une machine virtuelle **Turing-complète** qui exécute la logique implémentée dans les **smart contracts** et les transactions.
118	**Exchange**	Plateforme, souvent centralisée (**DEX** si distribuée), qui permet d'acheter, de vendre ou d'échanger des **cryptoactifs** contre d'autres **cryptoactifs** ou contre de la **monnaie** ayant **cours légal** (par exemple euro ou dollar). Un exchange assure généralement : la tenue de comptes clients, la gestion d'ordres (carnet d'ordres, prix au marché, etc.), la conservation des **actifs** dans des wallets de la plateforme. Contrairement à un **DEX**, l'exchange repose sur un intermédiaire qui opère l'infrastructure, applique les règles de conformité (**KYC**, **LCB-FT**) et, dans l'Union européenne, doit être enregistré ou agréé comme PSAN puis CASP au titre de MiCA.

F

119	**Farming**	Yield Farming / Farming. Pratique de la finance décentralisée (DeFi) consistant pour un utilisateur à placer des cryptoactifs dans un protocole (souvent des pools de liquidité, des plateformes de prêt/emprunt ou des stratégies automatisées) afin de recevoir des récompenses, généralement sous forme d'intérêts, de frais partagés ou de jetons de gouvernance. Le farming combine plusieurs sources de rendement (frais d'AMM, tokens bonus, intérêts de lending…) et peut impliquer des risques accrus : volatilité, impermanent loss, risques de smart contracts, ou défaillance des incitations économiques.
120	**Fiduciaire**	Voir **Monnaie fiduciaire**
121	**Finalité** *Finality*	Moment à partir duquel une transaction ou un **bloc** ne peut plus être annulé ni réorganisé dans le **registre distribué**.
122	**Finalité déterministe** *Deterministic Finality*	**Finalité** immédiate garantie dès qu'un bloc est validé par un **algorithme de consensus BFT**.
123	**Finalité probabiliste** *Probabilistic Finality*	**Finalité** obtenue lorsque la probabilité de réorganisation diminue avec le temps sans jamais devenir nulle (ex : Bitcoin).
124	**Finance Décentralisée** *Decentralized Finance*	Voir **DeFi**

125	**Flash loan attack**	Attaque utilisant des emprunts instantanés pour manipuler des protocoles.
126	**Flashbots**	C'est un organisme de recherche et développement (https://github.com/flashbots/pm) dont l'objectif est de réduire l'impact négatif des stratégies liées à la Miner Extractable Value (MEV), c'est-à-dire les bénéfices générés par le mineur grâce à un agencement spécifique des transactions de son bloc. Flashbots permet la mise en place de canaux de communication off-chain au travers desquels mineurs et utilisateurs peuvent s'entendre sur l'organisation des transactions du bloc. Ce système constitue une alternative aux enchères on-chain et contribue donc à réduire le prix moyen du gas.
127	**Fongibilité** *Fungibility*	La fongibilité qualifie le caractère interchangeable des **actifs** détenus. « La fongibilité implique droit de disposer et obligation de restituer seulement en équivalent » (Cour de Cassation). Dans le langage financier, la fongibilité peut s'appliquer aussi bien à des titres qu'à une monnaie. La fongibilité d'une **monnaie** signifie qu'elle peut être échangée à tout moment et au pair contre une autre **monnaie**, libellée ou non dans la même unité de compte. Les pièces et billets de banque sont fongibles et dans la même unité de compte. La fongibilité s'applique aussi à l'échange d'une **monnaie** divisionnaire ou d'un **actif** financier entre ses différentes divisions. La fongibilité s'applique aussi entre deux **monnaies** qui circulent simultanément, même avec des unités de comptes différentes : Lors du passage à l'euro, on a eu recours à la fongibilité entre **monnaies** nationales et l'euro, durant la phase de transition, pour accepter en même temps des **moyens de paiements** libellés en francs et en euros. La fongibilité est enfin l'impossibilité de différencier des **actifs** venant de transactions différentes au sein d'une même transaction.
128	**Fork**	De l'anglais fork, qui signifie embranchement ou fourche. Dans le cas d'une **blockchain** c'est un moyen de diverger le registre en 2 versions qui continueront à avancer séparément. Un fork a pour but de (1) Faire évoluer ou réparer la **blockchain** dans une nouvelle copie, ou bien (2) Lancer une nouvelle blockchain avec de nouveaux services se basant sur l'état de la première. Un hardfork ne garde pas de compatibilité avec la version antérieure alors qu'un softfork est rétro-compatible.
129	**Frontrunning**	Pratique consistant à placer une opération avant une autre opération connue à l'avance afin d'en tirer un avantage. Dans les systèmes **blockchain** et la **DeFi**, le frontrunning peut se produire via l'observation des transactions en attente (**mempool**) et la priorité donnée par les frais, ou via des mécanismes de réordonnancement par des intermédiaires (ex. recherche de valeur extractible).
130	**FTS**	Fabric Token SDK (Fabric Token Service). Une collection d'API et de services permettant aux développeurs de créer des applications décentralisées basées sur des tokens sur la plateforme **Hyperledger Fabric**. Utilise un modèle **UTXO** (Unspent Transaction Output) où chaque transaction consomme des tokens non dépensés et en crée de nouveaux
131	**Full node**	**Nœud** vérifiant l'intégralité des **blocs** et transactions, garantissant la sécurité du réseau.

132	**Fund**	Action consistant à créditer un compte, un **wallet**, un **smart contract** ou un jeton avec une certaine quantité d'**actifs** (**monnaie**, **stablecoins**, **jetons**). Dans le contexte de **l'Eurosystème**, le fund peut par exemple désigner le fait de créditer un Dedicated Cash Account (**DCA**) sur le module **RTGS** ou un Main Cash Account (**MCA**) sur **CLM**, afin de disposer de liquidités en **monnaie de banque centrale** pour le règlement de paiements ou d'**actifs tokenisés**. Dans les systèmes de tokenisation ou de **stablecoins**, fund correspond au dépôt de l'**actif** sous-jacent préalable à l'émission (**mint**) des jetons représentatifs.

G

133	**Gas**	Le gas est l'unité de compte utilisé dans le calcul des frais de transactions sur Ethereum : les transactions coûtent une quantité de gas variable selon leur complexité et reflétant la dépense électrique nécessaire aux mineurs pour les exécuter. Le coût final d'une transaction est alors égal au produit de la quantité de gas nécessaire à son exécution et du prix d'une unité de gas.
134	**Gas limit**	Quantité maximale de **gas** qu'une transaction est autorisée à consommer.
135	**Gas price**	Prix du **gas** fixé par l'utilisateur pour déterminer la priorité de la transaction.
136	**Genèse**	Bloc genèse, (genesis block) : premier bloc d'une **blockchain**, point de départ du registre. Il est "codé en dur" (ou défini à l'initialisation) et sert de référence pour enchaîner tous les blocs suivants. Il établit l'état initial du réseau (paramètres, règles, parfois soldes initiaux selon les systèmes). Exemple : le bloc 0 de **Bitcoin** est appelé "Genesis Block".
137	**Gouvernance on-chain** *On-Chain Governance*	La gouvernance on-chain est un système de gestion des changements de la **blockchain** où les règles régissant ce processus sont directement codées dans la **blockchain**. Ainsi, les développeurs proposent des modifications via des mises à jour de code et chaque **nœud** du réseau **blockchain** vote pour accepter ou rejeter la modification proposée.
138	**Governance token**	Jeton donnant des droits de vote dans la gouvernance d'un protocole.
139	**gRPC**	Cadre d'appels de procédures distants (**Remote Procedure Calls – RPC**) open source, utilisé pour faire communiquer des services entre eux à travers le réseau. gRPC s'appuie généralement sur HTTP/2 et des interfaces décrites avec Protocol Buffers, ce qui permet des échanges structurés, rapides et binarisés entre microservices, nœuds ou API. Il est fréquemment employé pour connecter des composants d'infrastructures distribuées (par exemple des services liés aux **technologies de registres distribuées**, aux **wallets** ou aux plateformes de **cryptopaiement**). Le terme « gRPCs » désigne la version sécurisée du gRPC sur TLS
140	**GSC**	Global **Stablecoin**
141	**Gwei**	Sous-unité d'Ether utilisée pour mesurer le coût du gas (1 gwei = 10^-9 ETH).

H

142	**Hachage**	Le hachage (de l'anglais hash, signifiant, recouper et mélanger) est une technique cryptographique utilisant une fonction à sens unique (irréversible) qui vise à condenser des données (un chiffre, une texte, un livre,…) dans une autre donnée de taille fixe permettant de garantir son intégrité. Voir Taux de hachage
143	**Halving**	Désigne le procédé périodique de division par 2 des récompenses des mineurs de certaines **blockchains** ayant un **mécanisme de validation** par la **preuve de travail** (**PoW**) et qui est au cœur des modèles économiques régissant ce type de **cryptomonnaies**. (Voir aussi **Minage**)
144	**Hard fork**	Un **fork** dans lequel on effectue modification non rétrocompatible entraînant la création de deux versions du protocole si tous les **nœuds** ne mettent pas à jour.
145	**Hash Timelock contracts**	*Voir* **HTLC**
146	**HD Wallet**	Les wallet déterministes hiérarchiques, également appelés HD wallet ou portefeuilles ensemencés de type 2, génèrent de nombreuses paires de clés publiques/privées à partir d'un point de départ unique : la seed. Les paires de clés sont dérivées dans une arborescence à la différence des wallets séquentiels où elles sont générées de manière linéaire.
147	**HFMM**	Hyperbolic Function Market Maker (3. AMM algorithm selection)
148	**HMAC**	Méthode d'authentification utilisant une fonction de hachage combinée à une clé secrète.
149	**HTLC**	Hash Time Lock Contract - HTLC **Smart Contract** permettant des échanges conditionnels entre **blockchain** sans tiers de confiance. L'interopérabilité est effectuée via une mise en séquestre de l'**actif** et basée sur une contrainte de temps, débloquant les **actifs** par un partage de secret entre les participants
150	**Hyperledger**	Hyperledger est un projet open-source lancé en 2015 par la fondation Linux ayant pour but de développer un ensemble d'outils et d'infrastructures de déploiement de **blockchains privées** dédiées aux entreprises. (Hyperledger Fabric)

I

151	**IBC** *Inter-Blockchain Communication*	Protocole d'interopérabilité permettant aux blockchains Cosmos d'échanger données et actifs.
152	**IBFT**	IBFT (Istanbul BFT). Istanbul Byzantine Fault Tolerance et un **algorithme de consensus** de type **BFT**, conçu pour les **blockchains permissionnés**, dans lequel un ensemble de validateurs doit approuver chaque **bloc** avant son inscription dans le **registre distribué**. IBFT garantit la finalité immédiate des blocs : une fois validé, un bloc ne peut plus être remis en cause. Ce mécanisme est utilisé dans plusieurs implémentations de **blockchains** d'entreprise.
153	**ICO**	De l'anglais Initial Coin Offering (ICO), signifiant offre initiale de **cryptoactifs**. Mécanisme qui permet le financement de projet se basant sur la **blockchain** par l'émission de **cryptoactifs** pendant la phase de démarrage. Deux types de **cryptoactifs** (également appelés tokens ou jetons) peuvent être émis : **utility tokens** et **security tokens**.
154	**IEO**	De l'anglais, Initial Exchange Offering (IEO), c'est un **ICO** s'effectuant sur une plateforme d'échange référencée pour financer un projet en émettant un **cryptoactif** contre des fonds provenant d'un portefeuille de **cryptoactifs** ou de **monnaies légales**.
155	**Immuabilité** *Immutability*	C'est le caractère de ce qui ne peut pas être changé, même avec l'accord des parties. L'immuabilité de l'information stockée sur une **blockchain** est un des principaux atouts de cette innovation.
156	**Impermanent loss**	Perte temporaire subie par les fournisseurs de liquidité due à la variation des prix.
157	**Interopérabilité**	Capacité pour plusieurs blockchains d'échanger des données ou des **actifs**.

J

158	**Jeton de Monnaie Electronique** *Electronic Money Tokens*	Ou encore E-money Token Voir EMT

159 **Jeton utilitaire**
Utility Token

Jeton (**cryptoactif**) émis lors d'une **ICO** donnant accès à un droit d'usage sous forme de services ou produits par le projet financé

K

160 **KYC**

Know Your Customer. Processus d'identification et de vérification de l'identité d'un client, exigé des prestataires financiers pour prévenir la fraude, le blanchiment et le financement du terrorisme. Le KYC inclut la collecte de documents officiels, la vérification de l'adresse, et l'analyse du profil du client. En Europe, cette obligation s'applique notamment aux PSAN, CASP, banques, PSP et plateformes d'exchange**.**

161 **KYT**

Know Your Transaction. Processus d'analyse et de surveillance des transactions pour détecter des comportements suspects, en complément du KYC.

Dans les services liés aux **cryptoactifs**, le KYT repose souvent sur des outils de **traçabilité on-chain** permettant d'identifier : les adresses à risque, les schémas de fraude, les mouvements associés à des entités sanctionnées, les tentatives de dissimulation (**mixers**, **tumbling**, **layering**).

L

162 **L2**

Layer 2. On appelle layer-2 des protocoles off-chain développés au-dessus d'une blockchain et permettant d'en améliorer la scalabilité et/ou d'y introduire de la confidentialité.

163 **Layer 0**

Infrastructure permettant l'interopérabilité ou la création de blockchains (ex : Polkadot, Cosmos).

164	**Layering**	Étape intermédiaire d'un processus de blanchiment d'argent, consistant à multiplier les opérations successives pour casser la **traçabilité** entre l'origine des fonds et leur destination finale. Dans le contexte des **cryptoactifs**, le layering peut inclure : l'utilisation de **mixers**, le passage par des plateformes **d'exchange** multiples, l'usage de **DEX**, des transferts fragmentés ou automatisés. L'objectif est d'obscurcir les pistes et de rendre difficile la reconstitution du cheminement des fonds.
165	**LCB-FT**	Lutte contre le blanchiment et le financement du terrorisme Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Cadre réglementaire français et européen visant à prévenir le blanchiment d'argent (LCB) et le financement du terrorisme (FT). Il impose des obligations aux banques, prestataires de services de **paiement** et prestataires sur **cryptoactifs** (en France **PSAN**, puis **CASP** au titre de **MiCA**) : **KYC**, **KYT**, surveillance des transactions, déclaration à TRACFIN, analyse des risques, gel des avoirs. La LCB-FT constitue le socle de conformité applicable aux services de paiement, aux **cryptoactifs** et aux activités financières traditionnelles.
166	**Ledger**	Voir **Registre distribué**
167	**Light client**	Nœud ne téléchargeant qu'une partie des données (preuves et entêtes) pour vérifier les transactions.
168	**Lightning Channel**	Canal de paiement permettant des transactions instantanées entre deux parties sans passer on-chain.
169	**Lightning Network**	Réseau de paiements rapides basé sur des canaux hors-chaîne pour Bitcoin.
170	**Liquid Staking**	Mécanisme permettant à un utilisateur de mettre des **cryptoactifs** en staking tout en recevant en échange un **jeton** liquide représentant sa position **stakée**. Ce jeton peut être utilisé dans la **DeFi** (prêts, **pools de liquidité**, **échanges**), tout en continuant à accumuler les récompenses de staking associées. Le liquid staking améliore la liquidité des **actifs** immobilisés mais expose l'utilisateur aux risques propres aux protocoles intermédiaires (**smart contracts**, **dépegging** des jetons dérivés, **slashing** indirect).
171	**Liquidation**	Vente forcée d'un collatéral lorsque un emprunteur ne respecte plus les exigences de ratio.
172	**Liquidity mining**	Récompense attribuée aux utilisateurs fournissant de la liquidité.

M

173	**Mainnet**	Désignation du réseau principal d'une blockchain sur lequel la valeur est transférée en opposition à d'autres réseaux de tests (*Voir* Testnet**)**
174	**Masse monétaire** *Money supply* *Money stock*	La masse monétaire est la quantité de **monnaie** en circulation dans un pays ou une zone monétaire. Au plan statistique, elle est appréhendée via des « agrégats monétaires » : ✦ M1, agrégat étroit et le plus liquide, qui comprend les billets et pièces en circulation ainsi que les dépôts à vue au-delà d'une nuit (overnight deposits) ✦ M2, agrégat intermédiaire qui inclut M1 et y ajoute les dépôts à terme de moins de deux ans et les dépôts à préavis de moins de trois mois ✦ M3, agrégat large qui inclut M2 et y ajoute les instruments négociables sur le marché monétaire dont le degré de liquidité est élevé tels que les parts d'OPCVM monétaires ou les certificats de dépôts. L'agrégat M0 inclut à la fois les espèces (billets et pièces), qui circulent auprès des acteurs économiques, et les réserves détenues par les banques auprès de la banque centrale. Il correspond à la masse monétaire maîtrisée directement par la banque centrale, d'où son appellation de « base monétaire ».
175	**MCA**	Main Cash Account. Compte principal de liquidité qu'un établissement de crédit détient dans **CLM**, le module central de **TARGET Services**. Le MCA regroupe la liquidité en monnaie de banque centrale et alimente les autres comptes dédiés, notamment les **DCA**, utilisés pour les règlements spécifiques (**RTGS**, T2S, TIPS). Le MCA constitue la source centrale de gestion de trésorerie dans **l'Eurosystème**.
176	**Mécanisme de validation** *Consensus mechanism*	Appelé aussi mécanisme de consensus, c'est le mécanisme par lequel tous les **nœuds valideurs** d'un **registre distribué** entérinent un nouveau bloc d'opérations. Différents mécanismes existent, voir **preuve de travail** (**PoW**) et **preuve d'enjeu** (**PoS**).
177	**Mempool**	Memory Pool : zone d'attente où les transactions valides, diffusées sur le réseau mais pas encore incluses dans un bloc, sont stockées temporairement par les nœuds. Les producteurs de blocs (**mineurs**/validateurs) sélectionnent généralement des transactions dans le mempool pour construire le prochain **bloc**, souvent en tenant compte de critères comme la priorité et les frais.
178	**Merkle proof**	Preuve permettant de vérifier qu'une donnée appartient à un Merkle tree sans révéler l'ensemble des données.
179	**Merkle tree**	Structure arborescente de **hachage** permettant de vérifier efficacement l'intégrité d'un ensemble de données.

180 **Metamask**

Metamask est un wallet déterministe hiérarchique prenant la forme d'une extension web (Chrome, Firefox, Brave, Edge) et permettant à l'utilisateur d'envoyer des requêtes à la **blockchain** depuis son navigateur. Le logiciel permet ainsi de stocker et transférer des fonds en **cryptoactifs** sur **Ethereum** mais également d'interagir avec des **smart contracts** déployés sur la plateforme. Il s'agit du portefeuille le plus populaire de l'écosystème **Ethereum**, bénéficiant de nombreuses années d'ancienneté et d'une base de plusieurs millions d'utilisateurs.

181 **MEV**

Miner extractable value (MEV). Désigne le profit qu'un mineur peut faire en ajoutant, supprimant ou réarrangeant les transactions au sein de son **bloc**.

182 **MiCA**

De l'anglais : Markets in **Crypto-Assets** Regulation. Règlement européen établissant un cadre harmonisé pour l'émission, l'offre au public et les services sur **cryptoactifs** au sein de l'Union européenne. Adopté en mai 2023 et entré en vigueur en juin 2023, MiCA s'applique progressivement à partir de 2024. Le règlement MiCA prévoit un agrément obligatoire pour les prestataires fournissant des services sur **cryptoactifs** (**PSCA**/**CASP**), dont les exigences sont proches de l'agrément optionnel du régime français. Les prestataires agréés en application de MiCA peuvent bénéficier du passeport européen et fournir leurs services dans tous les pays de l'UE. MiCA définit également des règles spécifiques pour certaines catégories de cryptoactifs, notamment les **EMT** et **ART** (réserves, gouvernance, droits de rachat), ainsi que des obligations de transparence (livre blanc) et de conduite de marché.

183 **Minage**
Mining

Étape du mécanisme de validation de type preuve de travail (PoW) qui récompense le nœud valideur ayant réussi à confirmer la validité d'un bloc de transaction sur une blockchain.

184 **Mint**

Opération par laquelle un protocole, une plateforme ou un émetteur crée de nouveaux jetons, généralement en contrepartie d'un dépôt d'actifs sous-jacents (ex : **monnaies**, collatéral, réserves). Le mint augmente l'offre totale d'un jeton.

Dans les **EMT** et **ART**, le mint est strictement encadré (exigences de réserves, gouvernance, **MiCA**).

185 **Mixers**

Services qui permettent de mélanger plusieurs flux de **cryptoactifs** afin de rendre plus difficile la **traçabilité** des fonds sur une **blockchain**. Un mixer reçoit des **cryptoactifs** de différentes origines, les combine en un seul ensemble puis renvoie des montants équivalents à de nouvelles adresses choisies par l'utilisateur. Bien qu'ils puissent être utilisés pour protéger la confidentialité, les mixers sont fréquemment associés à des stratégies de blanchiment, de dissimulation de provenance, ou de contournement des sanctions.

186 **MNBC**
CBDC

Monnaie numérique de banque centrale en anglais Central Bank Digital Currency (**CBDC**)
Étymologiquement, monnaie numérique émise par une banque centrale.
Elle peut prendre la forme d'une digitalisation de la **monnaie fiduciaire** sans nécessairement se substituer aux billets et aux pièces, mais ayant les mêmes attributs dans ce cas, on parlera d'une MNBC de détail (en anglais retail CBDC ou general purpose CBDC). Ou d'une **monnaie** réservée aux échanges de gros montants entre les acteurs bancaires et financiers et les banques centrales, et aux opérations financières ou de paiement internationales de gros montants, et dans ce cas, on parlera d'une MNBC de gros (Wholesale CBDC).

187	**Monnaie**	**Actif**, matériel ou immatériel, qui traditionnellement a trois fonctions : un moyen d'échange, une unité de compte et une réserve de valeur. Historiquement, une monnaie pouvait être accepté par consentement général ou entre les parties, ou imposé par décision réglementaire. Désormais, c'est un instrument financier émis par une banque centrale ou par un intermédiaire financier agréé par une autorité publique et soumis à la surveillance prudentielle. Elle prend le nom de devise en dehors de sa zone monétaire d'émission. La monnaie constitue une créance sur l'entité émettrice (donc inscrite au passif de cette dernière) Voir aussi ***devise***.
188	**Monnaie de banque centrale** *Central Bank Money*	**CeBM** pour Central Bank Money. **Monnaie** émise par une banque centrale (billets de banque et dépôts auprès de la banque centrale) Elle constitue un passif de celle-ci et peut être utilisée à des fins de règlement.
189	**Monnaie de banque commerciale** *Commercial Bank Money (CoBM)*	**Monnaie** émise par une banque. L'expression « banque commerciale » est historique et a été conservée, quel que soit le type d'établissement émetteur (banque commerciale, banque mutualiste, ou établissement émetteur à statut particulier). Elle constitue une créance sur la banque et figure à son passif (dépôt auprès de la banque) ; elle peut être utilisé à des fins de règlement.
190	**Monnaie électronique** *Electronic money*	Le Code monétaire et financier (article L315-1) définit la monnaie électronique en tant qu'« une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement (...) et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique »
191	**Monnaie Fiat** *Fiat Money*	Expression anglaise faisant référence à une **monnaie** adossée à l'État ayant la même dénomination et la même unité de compte que la monnaie nationale : les espèces sont une forme de fiat money. Ce terme anglais est repris parfois sans traduction pour critiquer les monnaies ayant **cours légal** car soutenue par l'État via une réglementation et n'étant pas fondées sur une valeur intrinsèque comme les monnaie marchandises (or, argent,...), ou comme les **cryptoactifs** sur leur valeur de la confiance dans les mécanismes cryptographiques et économiques qui les fondent.
192	**Monnaie fiduciaire (Espèces)** *Cash, Paper or Fiat Money*	Étymologiquement, un **moyen de paiement** dont la valeur repose sur la confiance que lui accordent les agents économiques. En pratique, il s'agit aujourd'hui des billets et des pièces émis par des autorités publiques (banques centrales ou Trésors nationaux) et bénéficiant du **cours légal**.
193	**Monnaie légale**	Étymologiquement : **monnaie** définie par la loi. Dénomination de la monnaie à laquelle la loi confère des privilèges. L'article L111.1 du Code monétaire et financier définit « La monnaie de la France est l'euro ».
194	**Monnaie merchandise** *Commodity Money*	Marchandise acceptée historiquement comme moyen d'échange. Principalement, l'or et l'argent, mais aussi d'autres marchandises, comme des fruits ou des coquillages.

195	**Monnaie numérique** *Digital money*	Ce terme est employé dans deux sens différents : Au sens large, il désigne un **actif numérique** qui remplit les trois fonction de la **monnaie** (unité de compte, moyen d'échange et réserve de valeur et qui répond à la réglementation et est soumis à la supervision. 2. Dans un sens plus étroit, il désigne les **cryptomonnaies** et les formes immatérielles de **monnaie** émises par les banques centrales ou les banques commerciales. *Voir* **monnaie numérique de banque centrale MNBC**
196	**Monnaie numérique de banque centrale** *Central Bank Digital Currency (CBDC)*	*Voir* **MNBC**
197	**Monnaie programmable** *Programmable money*	**Monnaie numérique** qu'il est possible d'enrichir d'attributs et de services, tels que de planifier les transactions, décider de leur échéance et les combiner avec des **smart contracts**.
198	**Monnaie scripturale** *Bank money*	**Monnaie** qui se matérialise par une inscription en compte dans les livres d'une entité émettrice et qui constitue une créance sur cette dernière. La monnaie scripturale comprend les avoirs en compte de la clientèle auprès des banques (**monnaie de banque commerciale**) et les avoirs des banques auprès de la banque centrale (réserves en **monnaie de banque centrale**).
199	**Monnaie virtuelle** *Virtual money*	**Monnaie**, stockée sur un support virtuel, électronique y compris magnétique, ou autre ..., soit sous forme d'un dispositif individuel portable soit sous forme d'un compte électronique géré sur un serveur à distance
200	**Moyen de paiement** *Payment Instrument*	Tout instrument permettant de transférer des fonds entre un débiteur et un créancier. Voir **paiement**.
201	**MPC Wallet** *Multi-Party Computation Wallet*	**Portefeuille** où la **clé privée** est répartie entre plusieurs parties effectuant des calculs collaboratifs.
202	**Multi-signature** *Multisig*	Mécanisme exigeant plusieurs signatures pour autoriser une transaction.

N

203	**NEAR sharding**	Division du réseau en fragments permettant une scalabilité horizontale.

204 **Nœud valideur**
Validating node

Système informatique qui participe à un **registre distribué**. Sur une **blockchain publique**, tous les nœuds sont valideurs et sont éligibles à autoriser l'ajout d'un nouveau bloc.

205 **Nonce**

De l'anglais Number used ounce. Dans un **mécanisme de consensus** Proof of Work (**PoW**), le nonce est un nombre à usage unique recherché par les mineurs afin de produire un hachage du **bloc** inférieur à la cible fixée par la difficulté du réseau. Le nonce n'a pas de signification particulière : il sert uniquement à varier l'entrée du calcul de hachage jusqu'à obtenir un résultat conforme aux règles du protocole. Comme il n'existe pas de méthode analytique pour le déterminer, la recherche du nonce se fait par force brute, ce qui nécessite un temps moyen appelé **temps de bloc**, dépendant de la **difficulté de minage**

O

206 **Off-chain**

Se dit d'une opération ou d'un traitement réalisé en dehors de la blockchain, souvent pour réduire les coûts, augmenter la rapidité ou préserver la confidentialité.
Les solutions off-chain peuvent ensuite publier une preuve ou un résultat sur la blockchain (ex. rollups, canaux de paiement, calcul externe), assurant un lien sécurisé entre l'environnement externe et l'état on-chain.

207 **On-chain**

Se dit d'une opération, d'un **smart contract**, d'un enregistrement ou d'un événement exécuté directement sur une **blockchain**, où il bénéficie des propriétés propres au **registre distribué** : immuabilité, transparence et vérifiabilité. Une transaction on-chain est validée par le réseau et inscrite dans le **ledger**, ce qui en garantit l'intégrité mais implique des coûts et des délais liés au protocole.

208 **Oracle**

Un oracle **blockchain** est une brique de confiance permettant de partager à un **smart contract** des données extérieurs à un écosystème **blockchain**.

209 **Oracle manipulation**

Attaque exploitant ou faussant les données envoyées par un oracle.

P

210	**Paiement**	Un paiement est une modalité d'extinction d'une créance née de la fourniture d'un produit ou d'un service, par un transfert monétaire entre un débiteur et un créancier. Une cession d'un actif numérique est une autre modalité de règlement de la créance.
211	**Parachain**	Blockchain indépendante reliée à la relay chain de Polkadot.
212	**PDC**	Private Data Collection (Collection de Données Privées) Un mécanisme dans **Hyperledger Fabric** qui permet à un groupe restreint d'organisations sur un canal de partager des données confidentielles, invisibles aux autres membres du canal. Les données privées sont stockées uniquement sur les pairs autorisés, tandis qu'un hash (empreinte) de ces données est inscrit sur le grand livre pour garantir l'intégrité sans divulguer le contenu.
213	**PoA**	Proof-of-Authority (PoA). Désigne un mode de consensus où seul un petit nombre d'acteurs possède le droit de valider les transactions.
214	**Polygon**	Polygon (anciennement Matic Network). Solution de scalabilité et écosystème multi-chaînes construit autour d'**Ethereum**, permettant des transactions plus rapides et moins coûteuses. Polygon combine : une sidechain **PoS** compatible **EVM**, des solutions Layer 2 (**ZK-Rollups**, zkEVM), des outils pour créer des **blockchains** dédiées (« supernets »). La monnaie interne est MATIC, utilisée pour les frais, le staking et la gouvernance. Polygon est largement utilisé pour les applications **DeFi**, les **NFT**, les jeux et les paiements.
215	**Pool de minage** *Mining Pool*	Groupement de **mineurs** qui mutualisent leur puissance de calcul (**hashrate**) afin d'augmenter la probabilité collective de trouver des **blocs** et de lisser les revenus. Les récompenses (récompense de bloc et/ou frais de transaction) sont ensuite réparties entre les participants selon leur contribution, via un mécanisme de partage défini par le pool.
216	**Portefeuille électronique** *e-Wallet*	Dispositif logiciel ou matériel permettant de stocker de manière numérique un ou plusieurs **moyens de paiement** électroniques (par exemple des cartes de paiement, des cartes prépayées ou des jetons de **monnaie électronique**) et de les utiliser de façon sécurisée pour des paiements de proximité ou en ligne. Un wallet de **cryptomonnaies** est un type particulier de portefeuille électronique qui gère un ou plusieurs couples de clés privées et de clés publiques, permettant de détenir et de signer des transactions en **cryptoactifs** ; il peut ainsi être associé à plusieurs adresses de réception pour un même utilisateur.
217	**PoS**	Voir **Preuve d'enjeu** de l'anglais Proof of Stake, c'est un **mécanisme de validation** se basant sur la mise en séquestre de **cryptoactifs** par les **noeuds valideurs** d'une **blockchain publique**.
218	**PoW**	Voir **Preuve de travail** de l'anglais, Proof of Work c'est le premier **mécanisme de consensus** sur blockchain utilisé d'abord par **Bitcoin**. Les **nœuds valideurs** consomment une énergie électrique pour le **minage** des blocs nécessitant donc un fort **taux de hachage** (**hashrate**).
219	**Preuve d'enjeu** *Proof of Stake*	Voir **PoS**

220	**Preuve de travail** *Proof of Work*	Voir **PoW**
221	**Preuves à divulgation nulle de connaissance** *Zero-Knowledge Proofs*	Voir **zk-Proofs**
222	**Problème des généraux Byzantins** *Byzantine Generals Problem*	Dilemme classique de l'informatique distribuée décrivant la difficulté pour plusieurs acteurs de parvenir à un accord fiable lorsque certains participants peuvent être défaillants ou malveillants. Ce problème illustre les défis de **consensus** dans un **registre distribué**, où les **nœuds** doivent s'entendre sur un même état malgré des messages incorrects, absents ou contradictoires. Les algorithmes de type **IBFT**, **QBFT** ou autres variantes de **tolérance aux fautes byzantines** (**BFT**) sont précisément conçus pour répondre à ce défi.
223	**Proxy contract**	Contrat intermédiaire permettant de déléguer l'exécution vers un autre **smart contract** afin de faciliter les mises à jour sans changer l'adresse initiale.
224	**PSAN**	**Prestataire de Services sur Actifs Numériques** (**PSAN**) / **Digital Asset Service Provider** (DASP) : statut français créé par la loi PACTE du 22 mai 2019 et codifié au CMF (chapitre « PSAN », art. L.54-10-1 à L.54-10-7). Un PSAN est une entreprise qui fournit, à titre professionnel, un ou plusieurs services sur actifs numériques (notamment : conservation pour compte de tiers, achat/vente contre monnaie ayant cours légal, échange contre d'autres actifs numériques, exploitation d'une plateforme de négociation, et autres services comme réception-transmission d'ordres, gestion de portefeuille, conseil, prise ferme, placement garanti/non garanti). L'exercice de certains services est soumis à enregistrement obligatoire auprès de Autorité des marchés financiers (AMF) et le régime prévoit aussi un agrément optionnel (plus exigeant), avec des obligations typiques de conformité (KYC/AML-CFT), de sécurisation et d'organisation/contrôle interne selon le périmètre de services. Repère chronologique UE : le règlement **MiCA** (UE 2023/1114) est entré en vigueur le 29 juin 2023 ; ses dispositions "**stablecoins**" s'appliquent depuis le 30 juin 2024 et le reste (dont l'agrément des prestataires au niveau européen, « **CASP** ») depuis le 30 décembre 2024 ; le PSAN correspond donc à un régime national avec des dispositions transitoires vers le cadre **MiCA**.
225	**PSCA** *CASP*	**Prestataire de services sur crypto-actifs** (**PSCA**) / **Crypto-Asset Service Provider** (**CASP**) : prestataire autorisé, au titre du règlement **MiCA** (UE 2023/1114), à fournir au sein de l'UE des services sur **cryptoactifs** (ex. conservation pour compte de tiers, exploitation d'une plateforme de négociation, échange, exécution/réception-transmission d'ordres, conseil, gestion, etc.). Le statut implique des exigences en matière d'organisation et de gouvernance, de protection des clients, de gestion des risques et de conformité (notamment LCB-FT), ainsi que des exigences prudentielles selon les services. **MiCA** est applicable depuis le 30 décembre 2024 (dispositions "**stablecoins**" applicables depuis le 30 juin 2024) et s'inscrit dans la convergence/remplacement progressif des régimes nationaux (ex. **PSAN** en France)

226 **PvP**

PvP (Payment versus Payment). Mécanisme de règlement garantissant que le paiement dans une devise n'est effectué que si le paiement correspondant dans l'autre devise a lieu simultanément. Le PvP vise à éliminer le risque de règlement principal dans les opérations de change (FX) : aucune des deux parties ne se retrouve exposée à avoir payé sa jambe de la transaction sans recevoir l'autre. Dans les systèmes de règlement modernes (y compris avec **actifs** ou monnaies tokenisés), le PvP peut être mis en œuvre via des infrastructures spécialisées ou des **smart contracts**, éventuellement en combinaison avec des **DCA** ou des comptes en **monnaie de banque centrale (wCeBM)**.

Q

227 **QBFT**

Quorum Byzantine Fault Tolerance (Quorum BFT) . Évolution moderne d'IBFT améliorant la robustesse, la performance et la flexibilité des chaines de blocs permissionnés. QBFT optimise les phases de validation pour réduire les risques de blocage et supporte des environnements où la gouvernance ou le nombre de validateurs peut évoluer. Cette variante est largement utilisée dans des plateformes basées sur Besu ou Quorum.

228 **Quorum**

Plateforme de **registre distribué** dérivée d'**Ethereum** et conçue pour des **blockchains permissionnés**, où les participants sont identifiés et autorisés. Quorum utilise la machine virtuelle Ethereum (**EVM**) et supporte des **algorithmes de consensus** adaptés aux environnements d'entreprise, tels que **IBFT** et **QBFT**, permettant une finalité rapide et une gouvernance maîtrisée. Cette solution est largement employée pour des cas d'usage institutionnels nécessitant confidentialité, contrôle des accès et compatibilité avec les outils de l'écosystème **Ethereum**.

R

229 **Ratio de Collatéralisation**
Collateral Ratio

Rapport entre la valeur du collatéral et le montant emprunté dans la DeFi.

230 **Reentrancy**

Vulnérabilité permettant à un **smart contrat** d'être réappelé avant la fin d'une transaction, provoquant des attaques.

231	**Registre distribué** *Distributed Ledger*	Registre électronique simultanément consulté, enregistré et synchronisé par des acteurs autorisés et qui évolue par l'addition chronologique de nouvelles informations préalablement validées par la totalité des acteurs. Ces informations sont **immuables** (destinées à ne jamais être modifiées ou supprimées)
232	**Registre unifié** *Unified Ledger*	Infrastructure intégrant **monnaie**, **actifs** et logique de **paiement** dans un même **registre** programmable. Ce concept est notamment porté par les travaux de la Banque des règlements internationaux (BRI) et exploré par l'**Eurosystème** dans le cadre des réflexions sur la tokenisation et l'évolution des infrastructures de règlement.
233	**Réserve de Liquidité** *Liquidity Pools*	Réserve de **jetons** déposés et immobilisés dans un **smart contract**, généralement au sein d'un protocole de finance décentralisée (**DeFi**). Cette réserve mutualisée sert de contrepartie pour permettre des échanges et/ou d'autres opérations, et les fournisseurs de liquidité peuvent recevoir une rémunération (frais et/ou incitations) en échange.
234	**Restaking**	Mécanisme permettant de réutiliser des **cryptoactifs** déjà placés en **staking** sur un protocole principal (par exemple **Ethereum**) afin de sécuriser d'autres services, chaînes, ou protocoles sans devoir immobiliser davantage de fonds. Le restaking délègue une partie de la sécurité économique fournie par les **validateurs** à des applications externes, tout en exposant les actifs mis en jeu à des risques supplémentaires de **slashing** si les obligations ne sont pas respectées. Des plateformes comme EigenLayer ont popularisé ce modèle dans les réseaux **PoS** avancés.
235	**Ripple**	Voir **XRP**
236	**Rollups**	Agrégation de plusieurs transactions hors de la **blockchain** principale puis enregistrement d'une seule transaction correspondante sur celle-ci. Technologie permettant de traiter un grand nombre de transactions en dehors de la **blockchain** tout en garantissant leur validité grâce à une preuve publiée sur la **blockchain**. Les rollups augmentent la capacité d'un réseau sans modifier son fonctionnement de base, car la vérification finale reste assurée par le **registre distribué** et par les **smart contracts** qui y sont déployés. On distingue principalement : les **zk-rollups**, qui reposent sur des **preuves à divulgation nulle** de connaissance, les **rollups optimistes**, fondés sur un mécanisme de vérification a posteriori (période de contestation).
237	**Rollups Optimistes** *Optimistic Rollups*	Solution d'extension qui traite les transactions hors de la **blockchain**, puis publie leurs données sur le réseau principal en supposant qu'elles sont correctes (« approche optimiste »). La validité peut être contestée pendant une période définie grâce à un mécanisme de preuve de fraude. Ce modèle permet de réduire les coûts et d'augmenter la capacité tout en conservant la sécurité du **registre distribué**.

238	**RTGS**	Real-Time Gross Settlement. Système de règlement brut en temps réel généralement géré par la banque centrale. Le module **TARGET** est le RTGS de la zone euro, utilisé pour les paiements de gros montant (**CeBM**) et les paiements critiques en monnaie de banque centrale. Chaque paiement est réglé individuellement, en temps réel, sans compensation, sur un **DCA**. RTGS assure la finalité immédiate des paiements dans **l'Eurosystème** et constitue le cœur du règlement interbancaire en euros.

S

239	**Schnorr signatures**	Schéma de signature efficace et agrégable, améliorant confidentialité et scalabilité.
240	**Script (Bitcoin)**	Langage simple basé sur une pile permettant de définir des conditions de dépense pour les **UTXO**.
241	**Sealevel (Solana runtime)**	Moteur d'exécution parallèle des smart contracts sur Solana.
242	**Security Token**	Jeton numérique représentant des **actifs** réels et réglementés (actions, obligations, immobilier, ...) C'est une classe de **cryptoactifs** émis sur un **registre distribué** dans le cadre d'un **STO**, représentant une valeur et pouvant donner accès à une rémunération sous forme pécuniaire.
243	**SegWit**	Segregated Witness : Amélioration de **Bitcoin** séparant les données de signature afin de réduire la taille des **blocs** et prévenir la malléabilité.
244	**Sel cryptographique**	Valeur aléatoire ajoutée à des données avant hachage pour prévenir les attaques par tables pré-calculées.
245	**Sharding**	Le sharding (partitionnement) est une technique permettant de fragmenter les données en "shards" afin d'améliorer les performances du réseau. Les **noeuds** d'une **blockchain** ne s'occupent que d'un shard au lieu de la totalité du **registre distribué** ou du réseau.
246	**Sidechain**	*Voir* **Chaine de blocs adjacente**
247	**Slashing**	Sanction appliquée aux **validateurs** malveillants ou négligents dans un système **PoS**.
248	**Slippage**	Écart entre le prix attendu et le prix réellement exécuté dans un échange.
249	**Slot**	Période courte durant laquelle un validateur peut proposer un **bloc**.
250	**Smart contract wallet**	**Portefeuille** où la logique de gestion (règles, signatures, limites) est codée dans un **smart contract**.
251	**Smart Contrat**	Ou 'smartcontrat' Voir **Contrat intelligent**

252	**Soft fork**	Un **fork** dans lequel on effectue une modification rétrocompatible des règles, permettant aux anciens nœuds d'accepter les nouveaux **blocs**.
253	**SOL**	Voir **Solana**
254	**Solana (SOL)**	**Blockchain publique** de couche 1 orientée haute performance, utilisant un mécanisme de **Proof of Stake** optimisé, combiné à d'autres techniques (notamment proof-of-history) pour atteindre des débits élevés et des coûts de transaction très faibles. Solana héberge des **smart contracts**, des **dApps** et de nombreux protocoles **DeFi** et **NFT**, en concurrence avec **Ethereum** sur certains cas d'usage. Caractéristiques principales : Inventeurs : Anatoly Yakovenko (fondateur principal), épaulé par Raj Gokal et l'équipe Solana Labs. Lancement : projet fondé en 2018, réseau lancé en 2020. Monnaie interne : SOL. **Turing-complet** : oui (smart contracts exécutés dans l'environnement d'exécution Sealevel). Langages principaux : Rust, C/C++ pour les programmes on-chain. Rang / market cap (2025) : dans le top 5–10 des **cryptoactifs** par capitalisation.
255	**Solidity**	Langage de programmation destiné à écrire des **smart contracts** exécutés sur l'Ethereum Virtual Machine (**EVM**). Inspiré de JavaScript, Python et C++, Solidity est le langage principal utilisé pour développer la majorité des protocoles **DeFi**, des **NFT**, des **ERC-20**, ERC-721, ERC-1155, ainsi que des applications déployées sur les **blockchains** compatibles **EVM** (**Polygon**, **BNB Chain**, **Avalanche** C-Chain, Arbitrum, Optimism, etc.) Solidity permet la gestion de structures complexes, la création d'événements, l'héritage multiple, et l'interaction avec d'autres contrats via l'ABI. Il est **Turing-complet**, et sa compilation génère du bytecode pour l'**EVM**.
256	**SPV**	Simplified Payment Verification: Méthode permettant de vérifier des transactions **Bitcoin** en utilisant seulement des entêtes et des **preuves Merkle**.
257	**Stable swap**	En **DeFi**, mécanisme d'échange optimisé pour les **actifs** de valeurs proches (**stablecoins**).
258	**Staking**	Mécanisme par lequel un utilisateur immobilise une quantité de **cryptoactifs** pour participer à la sécurité et au fonctionnement d'un réseau utilisant la **preuve d'enjeu** (**PoS**) ou des variantes apparentées. Les fonds placés en staking servent de garantie du bon comportement des validateurs : en contrepartie, l'utilisateur perçoit des récompenses (frais de transaction, émission monétaire, autres incitations) ; en cas de comportement fautif ou de non-respect des règles du protocole, une partie de la mise peut être confisquée (**slashing**). Le staking peut être effectué directement par l'utilisateur ou via des pools de staking, des plates-formes d'échange ou des solutions de **liquid staking** utilisées notamment en **DeFi**.
259	**State root**	Hachage représentant l'état complet de la **blockchain** à un instant donné, utilisé notamment dans **Ethereum**.

260 **STO**

De l'anglais **Security Token Offering** (STO). Levée de fonds consistant à émettre des **security tokens**, c'est-à-dire des jetons qui confèrent des droits de nature financière (par ex. droits économiques ou de gouvernance, créance, intérêts, participation à des revenus, parts assimilables à des titres). Contrairement à une **ICO** "utility", une **STO** relève d'un cadre réglementaire de type instruments financiers/valeurs mobilières (exigences d'information, distribution encadrée, KYC/LCB-FT, etc.), car le jeton est conçu pour représenter un investissement et des droits associés.

261 **Substrate**

Framework permettant de créer des blockchains modulaires (Polkadot).

262 **SushiSwap**

Exchange décentralisé (**DEX**) et protocole **DeFi** fondé initialement comme une variante de **Uniswap**, utilisant des **Automated Market Makers** (**AMM**) pour permettre le swap de **cryptoactifs** via des **pools de liquidité**. Les fournisseurs de liquidité déposent des **actifs** dans ces pools et reçoivent des frais de transaction, ainsi que, selon les modèles, des récompenses en jetons de gouvernance (**SUSHI**).
Fork de **Uniswap** datant de 2020, SushiSwap s'est développé en un écosystème plus large comprenant plusieurs produits **DeFi** (**DEX** multi-chaînes, **farming**, produits dérivés, etc.), déployés sur **Ethereum** et d'autres blockchains compatibles **EVM**.

263 **Sybil attack**

Attaque où un acteur crée de nombreux faux **nœuds** pour influencer ou perturber le réseau.

264 **Sybil resistance**

Propriété/mécanismes qui limitent ou neutralisent les **attaques Sybil** en rendant difficile, coûteux ou inefficace la création de nombreuses identités contrôlées par un même acteur (ex. **PoW**, **PoS**, exigences d'autorisation/identité, quotas, coûts économiques, règles de sélection/validation).

265 **Synthetic asset**

Actif numérique répliquant la valeur d'un actif réel ou d'un indice.

T

266 **Taproot**

Mise à jour de Bitcoin améliorant confidentialité, flexibilité des scripts et agrégation des signatures.

267	**TARGET Services**	Suite intégrée d'infrastructures de règlement de **l'Eurosystème**, gérée par la **BCE** et les **4CB**, permettant le règlement en monnaie de banque centrale des paiements, titres et liquidités. TARGET Services comprend notamment : **RTGS**, pour le règlement brut en temps réel des paiements de gros montant ; T2S, pour le règlement-livraison de titres en monnaie banque centrale ; TIPS, pour les paiements instantanés ; **CLM**, pour la gestion centralisée de la liquidité via les **MCA** et l'alimentation des **DCA**. ECMS pour la gestion du collatéral. Ces services constituent l'infrastructure de marché centrale de la zone euro et assurent la finalité, l'interopérabilité et la stabilité du règlement dans **l'Eurosystème**.
268	**Taux de hachage** *Hashrate*	Le taux de hachage est la vitesse avec laquelle un ordinateur effectue une opération de hachage dans le **minage** d'un bloc sur **blockchain**. Disposer d'un taux de hachage élevé est avantageux, car cela augmente les chances de miner le bloc suivant et d'obtenir la récompense.
269	**Technologie de registre distribué (DLT)** *Distributed Ledger Technology*	*Voir* **DLT**
270	**Testnet**	un testnet est un réseau utilisé par les développeurs afin de tester leurs applications. Un testnet possède quasiment les mêmes caractéristiques que le **mainnet** mais fonctionne avec des **cryptomonnaies** de test.
271	**Tether**	Tether (USDT) est un **stablecoin** indexé sur le dollar américain (1 USDT ≈ 1 USD), émis par Tether Holdings. USDT est utilisé massivement comme actif de référence et de liquidité sur les plateformes d'exchange et dans de nombreux protocoles **DeFi**. Caractéristiques principales : Devise de référence : USD (**peg** 1:1). Type : **stablecoin** centralisé, adossé à des réserves d'actifs financiers (cash, bons du Trésor, etc.) Lancement : 2014. Rang / market cap (2025) : plus grand **stablecoin** du marché, plus de la moitié de la capitalisation totale des **stablecoins.**
272	Tez	*Voir* **Tezos**
273	**Tezos**	Tezos **Blockchain publique** permettant la création de **smart contract**. Tezos propose une infrastructure permettant l'évolution de son protocole avec un système de vote sur la **blockchain**. L'**algorithme de consensus** utilisé par Tezos est un dérivé de la de la **proof-of-stake (PoS).** La **cryptomonnaie** interne à Tezos est appelée **Tez (XTZ)**
274	**Timestamp**	Horodatage associé à un **bloc** indiquant le moment où il a été validé par le réseau.

275	**Tokénisation**	La tokenisation d'un **actif** consiste à convertir les droits qui lui sont attachés en un enregistrement numérique. C'est une manière de représenter un **actif** réel (par exemple un bien immobilier, une obligation ou une propriété intellectuelle) dans le monde digital, et de pouvoir échanger cet **actif** en bénéficiant des mécanismes de la **blockchain**. Toute l'information liée à la détention de **l'actif** est tracée dans les **blocs** constituant la **blockchain**. Une fois enregistré sur la **blockchain**, le **token** peut donc être échangé au sein de la communauté.
277	**Traçabilité**	Dans le contexte des paiements, caractéristique d'un dispositif qui permet d'établir une piste d'audit pour conserver chacune des étapes d'un paiement. La **blockchain** apporte **l'immuabilité** et les preuves cryptographiques de cette piste d'audit afin de constituer un historique complet des transactions sur la **blockchain.**
278	**Travel Rule**	Obligation réglementaire imposant aux prestataires de services de paiement et aux acteurs des **cryptoactifs** de transmettre, lors d'un transfert de fonds ou de **cryptoactifs**, un socle minimal d'informations sur l'émetteur et le bénéficiaire (identité, coordonnées, parfois numéro de compte ou d'adresse). La Travel Rule vise à renforcer la **LCB-FT** en permettant l'identification et la **traçabilité** des flux entre intermédiaires (banques, PSP, **PSAN**, **CASP**, plateformes **d'exchange**) et à faciliter la détection des opérations suspectes dans les systèmes **KYC** / **KYT**.
279	**Treasury (DAO)**	Fonds collectifs gérés automatiquement par une **DAO**.
280	**Tumbling**	Technique de mélange de **cryptoactifs** proche des **mixers**, consistant à faire transiter des fonds à travers un grand nombre d'adresses intermédiaires ou de petites transactions successives. Le tumbling vise à fragmenter et réassembler les flux pour compliquer leur suivi. Cette méthode peut être utilisée comme étape du blanchiment d'argent, en particulier dans les schémas visant à dissimuler la provenance illicite de **cryptoactifs**.
281	**Turing-Complet**	En informatique, un système est Turing-complet s'il possède au moins les mêmes pouvoirs qu'une machine de Turing ou, autrement dit, s'il permet de représenter toutes les fonctions calculables au sens de Turing. Un langage de programmation Turing-complet permet d'implémenter des structures logiques complexes (boucles, itérations, etc) mais présente l'inconvénient d'offrir une surface d'attaque plus importante et l'impossibilité de prédire la finitude des programmes (boucle infinie) qui en découlent. Le script de programmation de Bitcoin n'est pas Turing complet mais solidity sur EVM l'est.
282	**TVL**	La Total Value Locked (TVL) est un indicateur utilisé dans le domaine de la DeFi afin de mesurer la taille et l'adoption d'un protocole. La TVL correspond à la valeur totale des **cryptoactifs** déposés par les utilisateurs dans un **smart contract**. En effet, la plupart des protocoles **DeFi** nécessitent un dépôt de collatéral pour pouvoir profiter des services proposés.

U

283 **Uniswap**

Exchange décentralisé (DEX) lancé en 2018, reposant sur un Automated Market Maker (AMM) permettant d'échanger des cryptoactifs sans carnet d'ordres. Les prix sont déterminés par une formule algorithmique (x·y=k) appliquée aux pools de liquidité fournis par les utilisateurs, qui reçoivent en échange des frais de transaction et des LP tokens. Uniswap est l'un des protocoles centraux de la DeFi avec son token UNI, déployé sur Ethereum et d'autres blockchains compatibles EVM.

284 **Upgradeability**

Capacité d'un **smart contrat** à être mis à jour sans changer d'adresse grâce aux **proxys**.

285 **USDC**

Stablecoin indexé sur le dollar américain (1 USDC ≈ 1 USD), émis par Circle et ses partenaires.
USDC est très utilisé par les acteurs institutionnels et dans la **DeFi**, avec un positionnement fort sur la transparence des réserves et la conformité.

Caractéristiques principales :

Devise de référence : USD (peg 1:1). Type : stablecoin centralisé, intégralement collatéralisé par des **actifs** libellés en USD (cash, T-bills). Lancement : 2018. Rang / market cap (2025) : deuxième stablecoin mondial par capitalisation.

286 **USDT**

Voir **Tether**

287 **UTXO**

Unspent Transaction Output (UTXO). Modèle de gestion des transactions utilisé notamment dans **Bitcoin**, où chaque opération consomme des sorties non dépensées (UTXO) provenant de transactions précédentes et en crée de nouvelles. Une transaction ne peut utiliser que des UTXO encore disponibles, ce qui garantit l'absence de double dépense et permet de vérifier facilement la validité de l'état du système.
Ce modèle s'oppose au modèle basé sur des comptes et des soldes, utilisé par d'autres **blockchains**.

V

288 **Validator set** Ensemble des validateurs autorisés à participer au consensus d'un réseau PoS.

289 **Vote on-chain** Système où les votes sont inscrits et comptabilisés directement sur la blockchain.

W

290 **Wallet** Dans notre contexte en paiements, correspond toujours à un portefeuille électronique. Voir e-Wallet

291 **wCeBM** Wholesale Central Bank Money *Voir* **Monnaie de banque centrale**

292 **Withdrawal key** Clé permettant de retirer les fonds mis en **staking**, distincte de la clé de validation.

X

293 **XRP** Cryptoactif natif du XRP Ledger (XRPL), un registre distribué open source conçu dès 2012 pour permettre des paiements internationaux rapides et peu coûteux. XRP est utilisé comme monnaie interne du réseau pour régler les frais de transaction et comme actif-pont entre différentes devises dans certaines solutions de paiements de Ripple. Le mécanisme de consensus du XRP Ledger n'est ni du PoW ni du PoS : il repose sur un protocole de consensus spécifique, dans lequel des validateurs indépendants parviennent à un accord toutes les quelques secondes, en s'appuyant sur des listes de nœuds de confiance (UNL – Unique Node List).

L'offre de XRP (100 milliards de jetons) a été pré-minée à la création du protocole, ce qui le distingue des cryptoactifs minés au fil du temps. En 2025, XRP fait partie des principaux cryptoactifs par capitalisation de marché, utilisé à la fois pour la liquidité sur les marchés et comme composant de certaines infrastructures de paiements et de remittances.

294 **XTZ** Voir **Tezos**

Y

295 **Yearn**

Yearn Finance: Plateforme DeFi spécialisée dans l'optimisation automatisée des rendements.
Les utilisateurs déposent des cryptoactifs dans des vaults (coffres) qui réallouent automatiquement les fonds entre différentes stratégies de yield farming, de prêt ou de fourniture de liquidité. Yearn vise à maximiser le rendement net en tenant compte des coûts, des risques et des opportunités de marché.

296 **Yield farming**

Voir **Farming**

Z

297 **zk-rollups**

Zero-Knowledge Rollups. Solution d'extension (scalabilité) qui exécute des transactions hors de la blockchain et en publie ensuite une preuve cryptographique garantissant que l'ensemble est correct. Cette preuve utilise des preuves à divulgation nulle de connaissance, ce qui permet d'assurer la validité des transactions sans en révéler le détail. (*Voir* zk-proofs)
Le réseau principal conserve ainsi la sécurité et l'intégrité de l'état, tout en réduisant fortement les coûts et le volume de données traitées.

298 **ZKP**

De l'anglais zk-Proofs ou Zero Knowledge Proof. Méthodes **cryptographiques** permettant de prouver qu'une affirmation est correcte sans révéler l'information qui permet de l'établir. Dans un protocole de zéro-connaissance, un vérificateur peut confirmer la validité d'un calcul ou d'une transaction sans accéder aux données sous-jacentes.
Ces techniques sont largement utilisées pour renforcer la confidentialité et la sécurité, notamment dans les **zk-rollups** et certains systèmes de **cryptopaiements**.
Exemple: Prouver que l'on possède plus de 3000€ sans révéler la somme exacte.