VOCABULAIRE DE LA CRYPTOMONNAIE

Souvent qualifiées de prometteuses, voire d'incontournables, les chaînes de blocs suscitent l'intérêt sur toutes les tribunes. Cette nouvelle technologie, sur laquelle reposent les cryptomonnaies, a le potentiel de révolutionner les façons de réaliser les échanges commerciaux, de sécuriser les données et de partager l'information.

L'émergence d'un champ de connaissances entraîne invariablement l'apparition de plusieurs nouveaux concepts et, par conséquent, la création de nombreux termes pour les désigner. Le domaine des chaînes de blocs et des cryptomonnaies ne fait pas exception et a engendré une pléthore de nouveaux termes (*minage*, *parachutage*, *bloc d'origine*, *registre distribué*), souvent imagés, pour illustrer de manière concrète des concepts plutôt intangibles.

Conscient du caractère novateur que revêt ce sujet, l'Office québécois de la langue française vous propose, avec la collaboration de l'Autorité des marchés financiers, de l'École de technologie supérieure ainsi que de l'Académie Bitcoin, un vocabulaire portant sur près d'une centaine de concepts, consacré à la terminologie des chaînes de blocs et de la cryptomonnaie. Un outil qui permettra à tous et toutes de discuter en français de l'émergence de cette technologie dans nos sociétés!

Symboles

Termes privilégiés

Termes utilisés dans certains contextes

Termes déconseillés

Ce vocabulaire est accessible en ligne à l'adresse suivante :
oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-cryptomonnaie.aspx.
Version PDF du 16 juillet 2024

Avertissement : Lors de la conversion du format HTML au format PDF, il est possible que certains caractères spéciaux ou signes typographiques (comme les espaces insécables) n'aient pas été correctement conservés. En cas de disparité, c'est la version en ligne du vocabulaire qui prévaut.

Index

A

algorithme de chiffrement, 1
algorithme de hachage, 2
application décentralisée, 3
arbre de Merkle, 4
argent électronique, 5
attaque par majorité, 6

B

bassin de transactions, 7
bloc, 8
bloc candidat, 9
bloc d'origine, 10
bloc orphelin, 11
bloc périmé, 12

C

capitalisation de marché, 13
capitalisation globale de marché, 14
chaîne de blocs, 15
chaîne secondaire, 16
cible de temps de hachage, 17
circuit intégré à application spécifique, 18
code de hachage, 19
consolidation, 20
contrat de minage, 21
contrat intelligent, 22
coopérative de minage, 23
correction, 24
creux sans précédent, 25
cryptoactif, 26
cryptomonnaie, 27
cryptomonnaie stable, 28
cryptomonnaie stable à garantie cryptomonétaire, 29
cryptomonnaie stable à garantie fiduciaire, 30
cryptomonnaie stable autorégulée, 31

D

division de la prime de minage, 32
double dépense, 33

E

embranchement accidentel, 34
embranchement convergent, 35
embranchement divergent, 36
empreinte numérique, 37
en-tête de bloc, 38
explorateur de blocs, 39
extensibilité, 40

F

feuille de route, 41
fonction de hachage cryptographique, 42
fongibilité, 43

H

hachage, 44
hauteur, 45

I

identifiant de bloc, 46
Internet des valeurs, 47

J

jeton, 48
jeton terni, 49

L

limite dissimulée, 50
limite supérieure, 51
livre blanc, 52

M

maillage de chaînes, 53
marché à la baisse, 54
marché à la hausse, 55
marché des capitaux, 56
mécanisme de validation, 57
minage, 58
minage clandestin, 59
minage infonuagique, 60
mineur, 61
monnaie, 62
monnaie fiduciaire, 63
monnaie virtuelle, 64

N

nœud, 65
nombre aléatoire, 66

Index

O

organisation autonome décentralisée, 67

P

parachutage, 68
plateforme d'échange décentralisée, 69
portefeuille multisignature, 70
première émission de jetons, 71
preuve d'activité, 72
preuve de capacité, 73
preuve de travail, 74
preuve d'enjeu, 75
preuve d'enjeu déléguée, 76
prime de minage, 77
profondeur, 78

R

racine de Merkle, 79
registre distribué, 80
réseau de test, 81
réseau principal, 82

S

seuil de hachage, 83
seuil minimal, 84
sommet sans précédent, 85
stockage à chaud, 86
stockage à froid, 87

T

taux de hachage, 88
témoin séparé, 89
temps de hachage moyen, 90

V

vol de cryptomonnaie, 91

Z

zone de résistance, 92
zone de support, 93

1. algorithme de chiffrement

Définition

Algorithme basé sur l'association entre une fonction mathématique et une clé de chiffrement, dont la séquence d'opérations conduit au chiffrement ou au déchiffrement de données.

Notes

Les algorithmes de chiffrement peuvent par exemple être utilisés afin de garantir l'intégrité des données, de confirmer l'identité d'un expéditeur ou d'assurer la confidentialité des éléments d'information transmis.

algorithme de chiffrement n. m.
algorithme de cryptage n. m.
algorithme cryptographique n. m.

Bien que l'utilisation de *cryptage* ait parfois été critiquée pour désigner le chiffrement, on constate que ce terme et ses dérivés tendent à se généraliser dans la documentation spécialisée.

anglais

cryptographic algorithm
crypto-algorithm
encryption algorithm
ciphering algorithm
encipherment algorithm

---

2. algorithme de hachage

Définition

Fonction mathématique qui permet la création d'une empreinte numérique en transformant un groupe de données de taille variable en un code unique de taille fixe.

algorithme de hachage n. m.

anglais

hash algorithm
hashing algorithm

---

3. application décentralisée

Définition

Application déployée sur le réseau décentralisé d'une chaîne de blocs, régie par un ou plusieurs contrats intelligents et généralement disponible en code source libre.

Notes

Les applications décentralisées sont notamment utilisées pour le financement participatif ou l'échange de cryptomonnaie contre des biens et services.

application décentralisée n. f.

anglais

decentralized application
Dapp
dApp
DApp

---

4. arbre de Merkle

Définition

Structure de données arborescente qui permet de condenser, au moyen d'une fonction de hachage cryptographique, un ensemble de blocs de données en un code de hachage simple et aisément vérifiable.

Notes

Dans le domaine des chaînes de blocs, et plus précisément dans celui de la cryptomonnaie, l'arbre de Merkle s'applique aux transactions contenues dans les blocs.

La structure de l'arbre de Merkle permet de contrôler la validité d'un ensemble de blocs de données sans avoir à valider individuellement chacun de ces blocs.

arbre de Merkle n. m.
arbre de hachage n. m.
arbre de hachage de Merkle n. m.

L'arbre de Merkle tire son nom de Ralph Merkle, qui a inventé ce type de structure à la fin des années 1970.

anglais

Merkle tree
hash tree
Merkle hash tree

---

5. argent électronique

Définition

Mode de paiement dont la valeur est stockée sur un support électronique.

Notes

On distingue deux formes d'argent électronique, selon le type de support électronique utilisé : l'argent stocké sur support matériel (une carte prépayée, par exemple) et l'argent stocké sur un support logiciel.

argent électronique n. m.
monnaie électronique n. f.
argent numérique n. m.
monnaie numérique n. f.

anglais

electronic cash
digital cash
electronic money
digital money
e-cash
e-money
digital currency

---

6. attaque par majorité

Définition

Cyberattaque ciblant les chaînes de blocs dont le fonctionnement repose sur la preuve de travail ou la preuve d'enjeu, par laquelle une personne ou un groupe prend le contrôle d'un réseau dans le but d'interférer avec les mécanismes de validation et de modifier le contenu de blocs existants.

Notes

Dans les cas des chaînes de blocs dont le fonctionnement repose sur la preuve de travail, l'attaque par majorité consiste à prendre le contrôle de plus de 50 % de la puissance de hachage d'un réseau, alors que pour les chaînes de blocs dont le fonctionnement repose sur la preuve d'enjeu, cette attaque consiste plutôt en la prise de possession de plus de 50 % du nombre total de jetons d'une cryptomonnaie.

Lors d'une attaque par majorité, il devient notamment possible pour les pirates informatiques d'annuler des transactions déjà autorisées afin de dépenser plus d'une fois les mêmes fonds (double dépense).

attaque par majorité n. f.

attaque des 51 % n. f.

Le terme *attaque des 51 %* n'a pas été retenu parce qu'il comporte une ambiguïté sémantique par rapport au rôle ainsi qu'à l'objet du pourcentage. En outre, une majorité peut correspondre à un pourcentage différent de 51 %, cette dernière valeur représentant essentiellement un seuil symbolique.

anglais

51% attack
51 percent attack
majority attack

---

7. bassin de transactions

Définition

Ensemble des transactions qui, dans une chaîne de blocs, sont en attente d'être validées par le réseau.

Notes

Dès lors qu'un nouveau bloc est validé et ajouté à la chaîne de blocs, les mineurs recourent au bassin de transactions afin de créer un nouveau bloc candidat à valider.

bassin de transactions n. m.

Le terme *bassin de transactions* a été proposé par l'Office québécois de la langue française en 2018 pour désigner ce concept.

anglais

memory pool
mempool
transaction pool

---

8. bloc

Définition

Ensemble de données liées à des transactions, dont la validité doit être confirmée au moyen d'un mécanisme de validation pour qu'il puisse être intégré à une chaîne de blocs.

Notes

En plus des données liées aux transactions, un bloc contient diverses métadonnées qui sont consignées dans son en-tête.

bloc n. m.

anglais

block

---

9. bloc candidat

Définition

Bloc qui est en attente d'une validation pour être intégré à une chaîne de blocs.

Notes

À la création d'un bloc, chaque nœud du réseau crée, à partir du bassin de transactions, un bloc candidat qu'il tente d'ajouter à la chaîne de blocs en recourant au mécanisme de validation utilisé par cette dernière.

bloc candidat n. m.

anglais

candidate block

---

10. bloc d'origine

Définition

Premier bloc d'une chaîne de blocs, auquel seront rattachés les blocs subséquents.

Notes

Le bloc d'origine est à la hauteur 0 puisqu'aucun bloc ne le précède.

bloc d'origine n. m.
bloc initial n. m.

anglais

genesis block
block 0
block zero

---

11. bloc orphelin

Définition

Bloc qui ne peut être rattaché à une chaîne de blocs parce que le registre du nœud qui le soumet ne contient pas l'intégralité des informations concernant le bloc précédent.

Notes

Une mise à jour du registre de l'utilisateur permet à ce dernier d'accéder aux données nécessaires pour valider le bloc en question.

Il ne faut pas confondre le bloc orphelin avec le bloc périmé, qui a été miné avec succès avant d'être invalidé.

bloc orphelin n. m.

anglais

orphan block

---

12. bloc périmé

Définition

Bloc qui est invalidé lors d'un embranchement accidentel parce qu'il ne fait plus partie de l'embranchement le plus long de la chaîne de blocs.

Notes

Les transactions contenues dans le bloc périmé sont réintégrées au bassin de transactions.

Il ne faut pas confondre le bloc périmé avec le bloc orphelin, qui ne peut être ajouté à la chaîne de blocs pour des raisons techniques.

bloc périmé n. m.

Le terme *bloc périmé* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais

stale block

---

13. capitalisation de marché

Définition

Évaluation d'une cryptomonnaie, calculée en multipliant le nombre total de jetons en circulation par leur valeur unitaire en monnaie fiduciaire.

capitalisation de marché n. f.
capitalisation marchande n. f.

anglais

market capitalization
market capitalisation
market cap

---

14. capitalisation globale de marché

Définition

Évaluation du marché des cryptomonnaies, calculée en additionnant les capitalisations de marché de toutes les cryptomonnaies existantes.

capitalisation globale de marché n. f.
capitalisation marchande globale n. f.

anglais

total market capitalization
total market capitalisation
total market cap

---

15. chaîne de blocs

Définition

Base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création.

Notes

La première chaîne de blocs est apparue avec les premiers bitcoins pour servir de registre des transactions et remplacer les intermédiaires entre acheteurs et fournisseurs de produits et de services. Ses champs d'application s'étendent à divers domaines comme par exemple les transports, la location, la santé, les banques.

chaîne de blocs n. f.

Le terme *chaîne de blocs*, calqué sur l'anglais, s'intègre au système linguistique du français. En effet, *chaîne* désigne un ensemble d'éléments successifs liés entre eux.

Le mot *chaîne* peut aussi s'écrire *chaine* en vertu des rectifications de l'orthographe (*chaine de blocs*).

anglais

blockchain

---

16. chaîne secondaire

Définition

Extension d'une chaîne de blocs, qui constitue un environnement autonome ayant ses règles propres.

Notes

La chaîne secondaire peut par exemple avoir une cible de temps de hachage différente de celle de la chaîne principale, tolérer un niveau de sécurité moindre ou encore recourir à un mécanisme de validation différent, par exemple à une preuve d'enjeu plutôt qu'à une preuve de travail. Une chaîne secondaire peut également viser à assurer l'extensibilité d'une cryptomonnaie en augmentant le nombre de transactions pouvant être validées à chaque instant.

chaîne secondaire n. f.

Le mot *chaîne* peut aussi s'écrire *chaine* en vertu des rectifications de l'orthographe (*chaine secondaire*).

anglais

sidechain

---

17. cible de temps de hachage

Définition

Période de temps visée par un protocole de chaîne de blocs pour la création d'un nouveau bloc.

Notes

Les protocoles de chaîne de blocs qui recourent à la preuve de travail comme mécanisme de validation ajustent régulièrement leur seuil de hachage afin que le temps de hachage moyen se rapproche de leur cible de temps de hachage.

La cible de temps de hachage a notamment une incidence sur la rapidité avec laquelle les transactions peuvent être confirmées par le réseau et sur la quantité de blocs périmés que génère la chaîne de blocs.

cible de temps de hachage n. f.

Le terme *temps de hachage moyen*, sur lequel est basé le terme *cible de temps de hachage*, a été proposé par l'Office québécois de la langue française en novembre 2018.

anglais

target block time
mining target

---

18. circuit intégré à application spécifique

Définition

Circuit intégré conçu et réalisé pour un nombre restreint d'applications, ce qui permet d'en optimiser l'utilisation.

Notes

Les possibilités des circuits intégrés à application spécifique sont multiples. Ces circuits sont notamment utilisés dans l'exécution de la fonction de hachage cryptographique pour le minage de blocs.

circuit intégré à application spécifique n. m.
circuit intégré spécifique n. m.
circuit spécifique n. m.
circuit intégré spécialisé n. m.

anglais

application-specific integrated circuit
ASIC

---

19. code de hachage

Définition

Code qui résulte de la transformation, au moyen d'une fonction de hachage cryptographique, d'un ensemble de données en une séquence alphanumérique de taille réduite, et qui permet d'identifier les données de départ sans y accéder.

Notes

La longueur du code de hachage dépend de l'algorithme de hachage utilisé.

Dans le domaine de la cryptomonnaie, le code de hachage permettant la validation d'un bloc est généralement désigné par le terme empreinte numérique.

code de hachage n. m.
code haché n. m.

anglais

hash code
hash

---

20. consolidation

Définition

Période de stabilisation des cours suivant de fortes fluctuations.

Notes

Les consolidations permettent de déterminer de nouvelles zones de support et de résistance.

consolidation n. f.

anglais

consolidation

---

21. contrat de minage

Définition

Contrat dans lequel sont définies les modalités d'un service de minage infonuagique.

Notes
Dans un contrat de minage, on définit notamment le type de matériel, la puissance de calcul allouée à l'investisseur, le prix ainsi que la durée de la location.

contrat de minage n. m.

anglais
mining contract

---

22. contrat intelligent

Définition
Programme dont le code est inscrit dans une chaîne de blocs et dans lequel est défini un ensemble d'instructions qui s'exécutent de manière automatique lorsque certaines conditions sont réunies.

Notes
Le plus souvent, les contrats intelligents visent à mettre en œuvre les clauses d'un accord entre plusieurs parties.

Les contrats intelligents peuvent notamment être utilisés dans le domaine du droit ou des assurances ainsi que pour le financement participatif. Par exemple, un contrat intelligent pourrait permettre d'indemniser automatiquement tous les passagers d'un vol qui a du retard.

contrat intelligent n. m.
contrat autoexécutant n. m.

smart contract

L'emprunt intégral à l'anglais *smart contract* n'est pas acceptable parce qu'il est employé depuis peu en français et qu'il ne s'intègre pas au système linguistique du français.

anglais
smart contract
cryptocontract
self-executing contract

---

23. coopérative de minage

Définition
Regroupement de mineurs qui mettent leurs ressources en commun par réseau afin d'augmenter les probabilités de validation d'un bloc.

Notes
Dans une coopérative de minage, même si un mineur ne parvient pas à valider un bloc, sa participation est quand même comptabilisée, puisqu'il est rémunéré sur une base régulière en fonction de la puissance de calcul qu'il partage.

coopérative de minage n. f.
groupe de minage n. m.

anglais

mining pool

---

24. correction

Définition

Chute soudaine et substantielle d'un cours ou d'un marché après une longue période de hausse.

Notes

Une correction se produit le plus souvent lorsqu'un cours ou un marché atteint un niveau anormalement élevé.

Une correction ne reflète généralement pas l'opinion des investisseurs, mais résulte plutôt de facteurs relatifs au fonctionnement du marché.

correction n. f.
repli technique n. m.

Le terme *repli technique* s'emploie le plus souvent pour parler du marché boursier.

anglais

correction

---

25. creux sans précédent

Définition

Plus bas niveau jamais atteint par le cours des valeurs d'un marché, d'un secteur, d'un titre ou d'une cryptomonnaie.

creux sans précédent n. m.
bas sans précédent n. m.

anglais

all time low
ATL

---

26. cryptoactif

Définition

Ensemble des valeurs dont les opérations sont enregistrées sur une chaîne de blocs.

Notes

Parmi les cryptoactifs, on compte notamment les cryptomonnaies, mais également d'autres unités de valeur, fondées sur la même technologie, qui permettent d'accéder à des services donnés ou qui font office de titre de propriété, par exemple.

cryptoactif n. m.

anglais

cryptoasset
crypto-asset

---

27. cryptomonnaie

Définition

Monnaie virtuelle utilisée pour des échanges de biens ou de services, de pair à pair, généralement de manière indépendante du système bancaire ou de toute politique monétaire, et dont l'émission et les transactions reposent sur la technologie des chaînes de blocs.

Notes

La plupart du temps, les cryptomonnaies sont échangées sur une plateforme d'échange décentralisée.

Le fonctionnement et la sécurité de la cryptomonnaie s'appuient généralement sur la cryptographie à clé publique et les fonctions de hachage cryptographique.

Apparu en 2009, le Bitcoin est l'une des cryptomonnaies les plus connues. Pour distinguer les autres cryptomonnaies du Bitcoin, on emploie parfois le mot-valise *altcoin*, formé à partir des mots anglais *alternative* et *coin*.

cryptomonnaie n. f.
monnaie cryptographique n. f.
monnaie chiffrée n. f.

Bien que l'utilisation de *cryptage* ait parfois été critiquée pour désigner le chiffrement, l'utilisation du préfixe *crypto-* est justifiée ici, puisque celui-ci fait référence à *cryptographie*. On constate, par ailleurs, que *cryptage* et ses dérivés tendent à se généraliser dans la documentation spécialisée.

anglais

cryptocurrency

---

28. cryptomonnaie stable

Définition

Cryptomonnaie dotée de divers mécanismes visant à stabiliser sa valeur.

Notes

Les cryptomonnaies stables se déclinent en cryptomonnaie stable à garantie fiduciaire, à garantie cryptomonétaire et autorégulée.

cryptomonnaie stable n. f.

anglais

stablecoin
price stable cryptocurrency

---

29. cryptomonnaie stable à garantie cryptomonétaire

Définition

Cryptomonnaie stable dont la valeur s'appuie sur la mise en réserve d'une quantité de jetons d'une autre cryptomonnaie dans le but de garantir, pour chaque jeton émis, une valeur corrélée à celle de l'actif de référence.

Notes

Pour compenser les déviations de sa valeur, ce type de cryptomonnaie stable agit sur les incitatifs économiques liés à la mise en réserve de jetons d'une autre cryptomonnaie.

cryptomonnaie stable à garantie cryptomonétaire n. f.

Le terme *cryptomonnaie stable à garantie cryptomonétaire* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais

crypto-collateralized stablecoin
crypto-backed stablecoin

---

30. cryptomonnaie stable à garantie fiduciaire

Définition

Cryptomonnaie stable dont la valeur s'appuie sur la mise en réserve, pour chaque jeton émis, d'une valeur équivalente de la monnaie de référence dans un établissement bancaire.

Notes

La mise en réserve de la monnaie fiduciaire agit à titre de garantie auprès des investisseurs contre une éventuelle dévaluation de la cryptomonnaie.

cryptomonnaie stable à garantie fiduciaire n. f.

Le terme *cryptomonnaie stable à garantie fiduciaire* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais

fiat-collateralized stablecoin
fiat-backed stablecoin

---

31. cryptomonnaie stable autorégulée

Définition

Cryptomonnaie stable qui recourt aux contrats intelligents pour maintenir un cours stable, en compensant automatiquement les déviations de sa valeur, par rapport à un actif de référence, par une augmentation ou une diminution du nombre de jetons en circulation.

cryptomonnaie stable autorégulée n. f.

Le terme *cryptomonnaie stable autorégulée* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais

algorithmic stablecoin
non-collateralized stablecoin
uncollateralized stablecoin
elastic stablecoin

---

32. division de la prime de minage

Définition

Réduction de moitié du montant de la prime versée aux mineurs pour la validation de blocs ou pour leur participation au réseau.

Notes

La division de la prime de minage est prévue par un algorithme imbriqué dans le fonctionnement des cryptomonnaies reposant sur la preuve de travail. Ce mécanisme permet de réduire périodiquement la vitesse à laquelle sont créés les nouveaux jetons jusqu'à ce que, à terme, le nombre des jetons en circulation atteigne la valeur maximale fixée lors de la création de la cryptomonnaie.

La division de la prime de minage peut être déclenchée notamment après le minage d'un nombre déterminé de blocs.

division de la prime de minage n. f.
division de la récompense de minage n. f.

anglais

halving
halvening

Le terme *halvening* a été formé par la contraction des termes *halving* et *happening*.

---

33. double dépense

Définition

Acte frauduleux perpétré lors d'une attaque par majorité, par lequel une personne ou un groupe modifie l'historique des transactions d'un réseau afin de pouvoir dépenser plusieurs fois les mêmes fonds.

double dépense n. f.

anglais

double-spending
double spending

---

34. embranchement accidentel

Définition

Dédoublement temporaire d'une chaîne de blocs, typiquement provoquée par la création simultanée ou quasi simultanée de deux blocs.

Notes

La nouvelle chaîne de blocs entre en compétition avec la chaîne d'origine; aussitôt qu'un bloc est ajouté à l'une des chaînes, l'autre est le plus souvent abandonnée par le réseau. Conséquemment, l'un des deux blocs à l'origine de l'embranchement accidentel deviendra périmé.

Un embranchement accidentel peut également être causé par une cyberattaque.

embranchement accidentel n. m.

anglais

accidental fork

---

35. embranchement convergent

Définition

Modification mineure du protocole d'une chaîne de blocs qui invalide un sous-ensemble de blocs et dont la mise en œuvre nécessite la mise à jour du registre de la majorité des nœuds.

Notes

Après un embranchement convergent, l'ancienne version du protocole de la chaîne de blocs reste compatible avec la nouvelle, mais seuls les blocs proposés par les mineurs ayant fait la mise à jour seront considérés comme valides.

L'embranchement convergent est notamment utilisé pour corriger un bogue ou un dysfonctionnement, ou pour ajouter de nouvelles fonctionnalités.

embranchement convergent n. m.
embranchement rétrocompatible n. m.

Les termes *embranchement convergent* et *embranchement rétrocompatible* ont été proposés par l'Office québécois de la langue française en 2018 pour désigner ce concept.

Les composés formés avec rétro- s'écrivent généralement sans trait d'union, sauf lorsque le mot qui le suit commence par i ou u, auquel cas il prend le trait d'union afin d'éviter un problème de prononciation.

anglais

soft fork
softfork

---

36. embranchement divergent

Définition

Modification majeure du protocole d'une chaîne de blocs, qui résulte d'un consensus et dont la mise en œuvre nécessite la mise à jour du registre de chacun des nœuds.

Notes

Après un embranchement divergent, l'ancienne version du protocole de la chaîne de blocs devient incompatible avec la nouvelle.

En l'absence de consensus au sein des nœuds, un embranchement divergent peut provoquer la création d'une nouvelle chaîne de blocs et, conséquemment, d'une nouvelle cryptomonnaie. Le cas échéant, les personnes qui possédaient des jetons de la cryptomonnaie d'origine recevront un nombre égal de jetons de la nouvelle cryptomonnaie.

embranchement divergent n. m.
embranchement rétro-incompatible n. m.

Les termes *embranchement divergent* et *embranchement rétro-incompatible* ont été proposés par l'Office québécois de la langue française en 2018 pour désigner ce concept.

Les composés formés avec rétro- s'écrivent généralement sans trait d'union, sauf lorsque le mot qui le suit commence par i ou u, auquel cas il prend le trait d'union afin d'éviter un problème de prononciation.

anglais

hard fork
hardfork

---

37. empreinte numérique

Définition

Séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message ou d'un fichier sans le révéler, dont la valeur unique est produite par un algorithme de hachage.

Notes

L'empreinte numérique est notamment utilisée pour valider l'intégrité d'un fichier téléchargé sur Internet, l'expéditeur d'un message ou les transactions de cryptomonnaies, ou encore pour le stockage des mots de passe par les fureteurs.

Par exemple, le destinataire valide le contenu d'un message reçu en calculant son empreinte numérique puis en la comparant à celle calculée par le destinateur avant l'envoi du message. Si les deux empreintes numériques sont identiques, le destinataire est assuré de son intégrité.

empreinte numérique n. f.
empreinte de hachage n. f.
valeur de hachage n. f.
condensé n. m.
condensat n. m.
somme de contrôle n. f.

On trouve également les termes *condensé du message*, *résumé de message* et *résumé du message*.

anglais

message digest
hash value
hash digest
fingerprint
cryptographic hash
cryptographic message digest

38. en-tête de bloc

Définition
Ensemble de métadonnées situé au début d'un bloc de données, qui fournit de l'information sur la nature de son contenu.

Notes
Dans les chaînes de blocs, la filiation entre les blocs est notamment assurée par la présence dans leur en-tête de métadonnées associées au bloc précédent.

en-tête de bloc n. m.

Le terme *en-tête de bloc* est souvent employé à tort au féminin. Voir, à ce sujet, l'article *Noms masculins employés indûment au féminin* de la *Banque de dépannage linguistique*.

anglais
block header

---

39. explorateur de blocs

Définition
Site Web qui permet à quiconque d'accéder librement à l'information liée à chacune des transactions ayant été réalisée au moyen d'une cryptomonnaie depuis sa création.

Notes
L'explorateur de blocs permet notamment de connaître les parties concernées par chacune des transactions ainsi que les montants échangés.

explorateur de blocs n. m.

anglais
block explorer
blockchain explorer

---

40. extensibilité

Définition
Capacité d'un réseau ou d'un système à s'adapter à une augmentation des besoins entraînée par une multiplication rapide des utilisateurs, sans incidence sur son fonctionnement ou ses performances, ni sur les coûts d'utilisation.

extensibilité n. f.

En France, le terme *extensibilité* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2003.

anglais
scalability

---

41. feuille de route

Définition

Document prenant généralement la forme d'un tableau, dans lequel sont présentés les principaux objectifs, les étapes importantes ainsi que l'échéancier d'un projet, et qui donne une vue d'ensemble de son développement.

Notes

Une feuille de route réaliste permet généralement de modérer les attentes des parties prenantes.

feuille de route n. f.
calendrier de lancement n. m.

anglais

roadmap

---

42. fonction de hachage cryptographique

Définition

Fonction mathématique qui, appliquée à un ensemble de données de départ, génère un code de hachage.

Notes

La fonction de hachage cryptographique implique que le moindre changement dans les données de départ entraîne une modification importante du code d'arrivée.

La longueur du code de hachage obtenu varie selon l'algorithme de hachage utilisé.

Dans le domaine de la cryptomonnaie, la fonction de hachage cryptographique est une fonction intégrale appliquée à divers composants du système : signature de transaction, preuve de travail, arbre de Merkle, etc.

fonction de hachage cryptographique n. f.
fonction de hachage n. f.
fonction de condensation n. f.

anglais

cryptographic hash function
cryptographic hashing function
hash function
hashing function

---

43. fongibilité

Définition

Caractère des valeurs qui, n'ayant pas d'identité individuelle, peuvent être substituées les unes aux autres sans que cela affecte leur usage éventuel.

Notes

Par exemple, on considère comme des biens fongibles les monnaies, les matières premières et les produits de leur première transformation, certains produits agricoles de base ainsi que certaines productions industrielles de série.

Même si les monnaies sont généralement fongibles, ce n'est pas obligatoirement le cas pour les cryptomonnaies. En effet, lorsque l'historique des transactions est public, il est possible de repérer les jetons susceptibles d'être issus de transactions illicites (jetons ternis). Conséquemment, ceux-ci sont parfois bloqués sur les plateformes d'échange et perdent leur fongibilité.

fongibilité n. f.

anglais

fungibility

---

44. hachage

Définition

Opération qui consiste à appliquer une fonction mathématique à un groupe de données de taille variable afin de générer un code unique de taille fixe, que l'on utilisera pour l'authentification et le stockage d'information.

Notes

Le hachage est notamment utilisé dans le domaine de la cryptomonnaie pour la compression de données relatives aux blocs de transactions à enregistrer sur une chaîne de blocs.

hachage n. m.

anglais

hashing
hash coding

---

45. hauteur

Définition

Valeur fixe attribuée à un bloc, qui correspond au nombre de blocs le précédant dans une chaîne de blocs, jusqu'au bloc d'origine.

Notes

Il ne faut pas confondre la hauteur d'un bloc avec sa profondeur, celle-ci correspondant plutôt au nombre de blocs qui le suivent.

hauteur n. f.
hauteur de bloc n. f.

anglais

block height
block chain height
height

46. identifiant de bloc

Définition

Signature numérique qui est générée lors de la création d'un bloc par le hachage de son en-tête.

Notes

L'identifiant d'un bloc est toujours incorporé à l'en-tête du bloc suivant. C'est cette filiation entre les blocs qui est à l'origine de l'analogie avec la chaîne dans le terme *chaîne de blocs*.

identifiant de bloc n. m.
identifiant n. m.

anglais

block hash
hash
block identifier
block header hash
block ID

47. Internet des valeurs

Définition

Web caractérisé par la traçabilité des actifs numériques, et qui est doté d'outils permettant leur stockage, leur protection, leur gestion et leur échange sans intermédiaire.

Notes

La traçabilité, rendue possible par la technologie des chaînes de blocs, empêche la reproduction des actifs numériques, leur permettant ainsi de préserver leur valeur.

L'Internet des valeurs permet l'échange d'actifs numériques tels que l'argent, l'électricité, la propriété intellectuelle, la musique, les actions ou encore les titres.

Internet des valeurs n. m.
IdV n. m.

anglais

Internet of value
IoV

48. jeton

Définition

Unité de valeur fondamentale d'une cryptomonnaie, généralement utilisée pour les paiements ou pour accéder aux services des applications décentralisées.

Notes
La valeur d'un jeton d'une cryptomonnaie donnée fluctue selon l'offre et la demande.

jeton n. m.
cryptojeton n. m.

On emploie parfois le terme plus général *cryptomonnaie* pour désigner le présent concept.

anglais
coin
crypto-coin
token
crypto-token

Alors qu'on utilisait à l'origine *coin* pour désigner les jetons d'une chaîne de blocs primaire et *token* pour les jetons d'une chaîne secondaire, aujourd'hui, on emploie plus spécifiquement *coin* (ou *crypto-coin*) lorsqu'il s'agit de paiement, et *token* (ou *crypto-token*) lorsqu'il s'agit d'accéder aux services offerts par les applications décentralisées.

---

49. jeton terni

Définition
Jeton dont l'historique des transactions permet de l'associer à des opérations illicites.

Notes
L'utilisation d'un jeton terni est susceptible d'occasionner des complications pour son détenteur sur les plateformes d'échange.

Certaines cryptomonnaies ne donnent pas d'accès public à l'historique des transactions; leurs jetons ne peuvent donc pas être ternis.

jeton terni n. m.

Le terme *jeton terni* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais
tainted coin

---

50. limite dissimulée

Définition
Seuil minimal ou limite supérieure dont la valeur n'est révélée qu'après le lancement de la première émission de jetons.

Notes
En empêchant les plus gros investisseurs de se faire une idée de la fraction que représente leur investissement par rapport au montant total de la première émission de jetons, l'emploi d'une limite dissimulée permet de favoriser les plus petits investisseurs.

limite dissimulée n. f.
limite non dévoilée n. f.

Les termes *limite dissimulée* et *limite non dévoilée* ont été proposés par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais
hidden cap

---

51. limite supérieure

Définition

Somme maximale qu'une équipe souhaite amasser lors d'une première émission de jetons afin de mener à bien un projet.

Notes

L'atteinte de la limite supérieure met généralement fin à la collecte de fonds; les fonds excédentaires sont alors retournés aux investisseurs.

limite supérieure n. f.
plafond d'investissement n. m.

anglais

hard cap

---

52. livre blanc

Définition

Document formel présentant l'objectif général et les principales étapes du lancement d'une cryptomonnaie, le plus souvent publié entre l'annonce du projet et la première émission de jetons, afin de convaincre les investisseurs potentiels de son intérêt.

Notes

On trouve généralement dans un livre blanc une présentation de l'équipe ayant participé au projet, un organigramme, la structure de l'offre initiale de jetons, le prix initial du jeton, le nombre total de jetons, les risques et les avantages du projet, les dates importantes ainsi que plusieurs éléments d'ordre technique et juridique.

livre blanc n. m.

anglais

whitepaper
white paper

---

53. maillage de chaînes

Définition

Procédé qui consiste à relier deux chaînes de blocs afin de permettre la circulation de cryptomonnaie entre elles.

Notes

Les transactions effectuées entre deux chaînes de blocs maillées sont consignées dans le registre de chacune des chaînes de blocs.

maillage de chaînes n. m.

Le terme *maillage de chaînes* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept. Dans ce terme, *maillage* est employé par analogie avec son acception spécialisée en marine, où il signifie « action de relier deux chaînes entre elles (à l'aide d'une manille) ».

anglais

chain linking

---

54. marché à la baisse

Définition

Marché ou secteur caractérisés par une baisse prolongée du cours des valeurs, reflétant le pessimisme et la méfiance des investisseurs.

marché à la baisse n. m.
marché baissier n. m.

anglais

bear market
bearish market

---

55. marché à la hausse

Définition

Marché ou secteur caractérisés par une hausse prolongée du cours des valeurs, reflétant l'optimisme et la confiance des investisseurs.

marché à la hausse n. m.
marché haussier n. m.

anglais

bull market
bullish market

---

56. marché des capitaux

Définition

Marché sur lequel les agents économiques négocient entre eux leurs ressources en capitaux.

Notes

On parlera plus précisément de marché monétaire lorsque sont négociés des actifs très liquides, et de marché financier lorsqu'il s'agit d'instruments à long terme.

marché des capitaux n. m.

anglais

capital market

---

57. mécanisme de validation

Définition

Mécanisme qui vise à assurer la validité des blocs ajoutés sur une chaîne de blocs ainsi que les transactions qu'ils contiennent.

Notes

La preuve de travail, la preuve d'enjeu et la preuve d'activité sont des exemples de mécanismes de validation. Ces mécanismes reposent notamment sur la résolution de problèmes cryptographiques complexes ou sur la mise en garantie d'une quantité donnée de cryptomonnaie.

mécanisme de validation n. m.
protocole de validation n. m.
mécanisme de consensus n. m.
protocole de consensus n. m.

anglais

consensus mechanism
validation mechanism
consensus protocol

---

58. minage

Définition

Opération qui repose sur un mécanisme de validation et permet l'ajout de blocs à un réseau de cryptomonnaie, en échange d'une prime de minage.

minage n. m.
cryptominage n. m.

En France, le terme *minage* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2017.

forgeage n. m.

Le terme *forgeage* (en anglais, *forging* ou *minting*) est employé par certains pour désigner plus précisément une validation qui repose sur le mécanisme de la preuve d'enjeu, mais cette distinction n'est pas généralisée.

anglais

mining
cryptomining
forging
minting

---

59. minage clandestin

Définition

Pratique consistant à infiltrer un ordinateur ou un appareil mobile et à en détourner les capacités de calcul afin de miner une cryptomonnaie à l'insu de son propriétaire.

Notes
Bien que le minage clandestin ne vise pas à porter atteinte à l'appareil piraté, il peut néanmoins en ralentir grandement les performances de même qu'entraîner une hausse considérable des dépenses énergétiques liées à son utilisation.

minage clandestin n. m.
minage furtif n. m.

anglais
cryptojacking
drive-by mining
drive-by cryptomining
stealth mining

---

60. minage infonuagique

Définition
Minage effectué par l'intermédiaire d'une puissance de calcul louée à une société possédant un centre de données, et ce, pendant une durée généralement prédéterminée.

Notes
Le minage infonuagique permet de miner une cryptomonnaie sans avoir à composer avec les désavantages liés au matériel : le bruit, la chaleur, l'entretien des installations et les coûts engendrés par la consommation d'électricité.

Les modalités du minage infonuagique sont définies dans un contrat de minage.

minage infonuagique n. m.

anglais
cloud mining

---

61. mineur, mineuse

Définition
Personne qui valide et sécurise, par bloc, les transactions d'un réseau de cryptomonnaie en utilisant un mécanisme de validation.

Notes
Pour chaque bloc validé, les mineurs obtiennent une prime de minage.

mineur n. m.
mineuse n. f.
cryptomineur n. m.
cryptomineuse n. f.

forgeur n. m.
forgeuse n. f.

Les termes *forgeur* et *forgeuse* (en anglais, *forger* ou *minter*) sont employés par certains pour désigner plus précisément une personne qui valide un bloc au moyen d'une preuve d'enjeu, mais cette distinction n'est pas généralisée.

anglais

miner
cryptominer
forger
minter

---

62. monnaie

Définition

Instrument de mesure et de réserve de valeur, servant de moyen d'échange.

Notes

Lorsque la valeur de la monnaie est garantie par un État, on parle plus précisément de monnaie fiduciaire.

monnaie n. f.

Par extension, le terme générique *monnaie* désigne aussi les monnaies dématérialisées telles que les monnaies virtuelles.

anglais

money
currency

---

63. monnaie fiduciaire

Définition

Monnaie dont la valeur est déterminée par la confiance que lui accordent ses utilisateurs plutôt que par son coût de production.

Notes

La monnaie fiduciaire, qui comprend notamment les pièces et les billets de banque, n'a aucune valeur intrinsèque.

La valeur légale de la monnaie fiduciaire est garantie par l'État.

monnaie fiduciaire n. f.
monnaie à cours forcé n. f.

Le terme *monnaie à cours forcé* tire son nom du fait que l'utilisation de la monnaie fiduciaire est généralement imposée par l'État.

anglais

fiat money
fiat currency
fiduciary money
fiduciary currency

On établit parfois une distinction entre *fiat money* (ou *fiat currency*), qui met l'accent sur le caractère imposé par l'État d'une monnaie, et *fiduciary money* (ou *fiduciary currency*), qui insiste plutôt sur le fait qu'une monnaie tire sa valeur de la confiance que lui accordent ses utilisateurs.

---

64. monnaie virtuelle

Définition
Monnaie déployée dans un espace virtuel.

Notes
Certaines monnaies virtuelles, telles les cryptomonnaies, sont dites convertibles et peuvent être échangées contre une monnaie fiduciaire, et vice-versa.

La valeur légale des monnaies virtuelles n'est généralement pas garantie par l'État.

Plusieurs jeux vidéo intègrent une monnaie virtuelle utilisée à des fins ludiques pour acheter des accessoires aux personnages ou débloquer des fonctionnalités, par exemple.

monnaie virtuelle n. f.
argent virtuel n. m.
cybermonnaie n. f.
cyberargent n. m.

Le terme *monnaie virtuelle* et ses synonymes sont parfois employés de manière générique pour désigner toute monnaie stockée sur un support électronique.

anglais
virtual money
virtual currency
virtual cash
cybercash
cybermoney

---

65. nœud

Définition
Appareil informatique relié au réseau qui héberge une chaîne de blocs, destiné à relayer les transactions effectuées et à maintenir une copie complète ou partielle du registre distribué sur lequel ces transactions sont enregistrées.

Notes
Certains nœuds sont également destinés à valider les transactions.

nœud n. m.

anglais
node

---

66. nombre aléatoire

Définition
Séquence numérique générée de manière aléatoire, qui est utilisée lors de la validation d'un bloc candidat dans les chaînes de blocs dont le fonctionnement repose sur la preuve de travail.

Notes

Pour valider un bloc candidat, le mineur hache les données présentes dans l'en-tête du bloc afin d'arriver à un code de hachage dont la valeur est égale ou inférieure au seuil de hachage. Le nombre aléatoire est la seule donnée de cet en-tête qui varie à chaque tentative de validation.

nombre aléatoire n. m.
nombre aléatoire à usage unique n. m.

anglais

nonce

Nonce provient étymologiquement du nom *nanes* qui était employé au 13e siècle en moyen anglais. Il est aujourd'hui employé en linguistique dans l'expression *nonce word* qui désigne un « néologisme créé pour un usage unique ». L'idée que le terme *nonce* est l'abréviation de *number used once* est issue d'un phénomène d'étymologie populaire.

---

67. organisation autonome décentralisée

Définition

Organisation n'ayant aucun propriétaire, dont la gestion est automatisée selon un ensemble de contrats intelligents et pour laquelle la participation humaine est limitée ou inexistante.

Notes

Les règles qui régissent de manière automatisée le fonctionnement de l'organisation autonome décentralisée sont transparentes et immuables puisqu'elles sont formalisées par des contrats intelligents, qui sont eux-mêmes inscrits dans une chaîne de blocs.

Une organisation autonome décentralisée pourrait, par exemple, répartir automatiquement un budget entre plusieurs propositions de projets en faisant voter les parties prenantes à partir de contrats intelligents.

organisation autonome décentralisée n. f.
OAD n. f.

anglais

decentralized autonomous organization
DAO

---

68. parachutage

Définition

Opération promotionnelle consistant à distribuer gratuitement des jetons d'une cryptomonnaie, pendant une période définie, dans le but d'en augmenter le nombre de détenteurs ainsi que la visibilité d'un projet en démarrage.

Notes

La distribution des jetons se fait parfois en échange de services rendus, par exemple en contrepartie d'un partage d'informations sur les réseaux sociaux afin de promouvoir un projet en démarrage.

parachutage n. m.
largage n. m.

anglais

airdrop

---

69. plateforme d'échange décentralisée

Définition

Plateforme d'échange de cryptomonnaie déployée sur le réseau décentralisé d'une chaîne de blocs et qui permet une négociation directe entre personnes.

Notes

La plateforme d'échange décentralisée sert à jumeler des utilisateurs qui souhaitent échanger un type de cryptomonnaie contre un autre type de cryptomonnaie ou contre une monnaie traditionnelle, et inversement.

plateforme d'échange décentralisée n. f.

Au pluriel, on écrira : *des plateformes d'échange décentralisées*.

anglais

decentralized exchange platform
decentralized exchange
DEX

---

70. portefeuille multisignature

Définition

Portefeuille virtuel pour lequel deux clés privées ou plus sont nécessaires pour effectuer toute opération de retrait.

Notes

Le portefeuille multisignature permet de diviser la responsabilité de la possession des fonds, et apporte un échelon de sécurité supplémentaire.

Le fonctionnement du portefeuille multisignature est similaire à celui d'un compte indivis.

portefeuille multisignature n. m.

Les mots formés avec le préfixe *multi-* ne prennent pas de trait d'union, sauf lorsque le second élément commence par la voyelle i.

Bien que *multi-* signifie « plusieurs », les mots formés avec ce préfixe suivent la règle générale d'accord du pluriel : ils s'écrivent sans *s* au singulier et avec *s* au pluriel. On écrira donc : *un portefeuille multisignature* et *des portefeuilles multisignatures*.

anglais

multisig wallet
multi-signature wallet

---

71. première émission de jetons

Définition

Campagne de financement par laquelle un organisme vend une part des jetons de sa cryptomonnaie durant la phase de démarrage de son projet.

Notes

Même si les jetons vendus sont généralement utilisés pour acquérir le droit d'utilisation d'un service offert par l'organisme, ils peuvent parfois constituer des parts de l'entreprise émettrice.

première émission de jetons n. f.
offre initiale de jetons n. f.

anglais

initial coin offering
ICO
coin sale
initial token offering
ITO
token sale

Alors qu'on utilisait à l'origine *coin* pour désigner les jetons d'une chaîne de blocs primaire, et *token* pour les jetons d'une chaîne secondaire, aujourd'hui, on emploie plus spécifiquement *coin* lorsqu'il s'agit de paiement, et *token* lorsqu'il s'agit d'accéder aux services offerts par les applications décentralisées.

---

72. preuve d'activité

Définition

Mécanisme de validation en deux étapes, qui repose d'abord sur le minage d'un nouveau bloc qui ne contient qu'un en-tête, puis sur sa validation par un groupe de mineurs actifs sélectionnés au hasard.

Notes

Dans la preuve d'activité, un bloc n'est validé que lorsque l'ensemble des mineurs du groupe y apposent leur signature.

Une fois l'en-tête de bloc validé, les transactions y sont annexées.

La preuve d'activité peut être vue comme un mécanisme de validation hybride faisant appel à la preuve de travail et à la preuve d'enjeu.

preuve d'activité n. f.

anglais

proof of activity
PoA

---

73. preuve de capacité

Définition

Mécanisme de validation qui repose sur la mise à disposition d'un espace de stockage sur lequel sont enregistrées des séquences de nombres aléatoires utilisées pour la création de nouveaux blocs.

Notes
Plus la capacité de stockage disponible est grande, plus le nombre de solutions possibles stockées sera important. Ainsi, seul le mineur qui possède le nœud sur lequel se trouve la solution est récompensé pour la création du bloc.

preuve de capacité n. f.
preuve d'espace n. f.

anglais
proof of capacity
PoC
proof of space
PoSpace

---

74. preuve de travail

Définition
Mécanisme de validation de transactions qui repose sur la résolution d'un problème cryptographique complexe.

Notes
La preuve de travail mène notamment à l'ajout d'un bloc à une chaîne de blocs.

preuve de travail n. f.

En France, le terme *preuve de travail* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2017.

anglais
proof of work
PoW

---

75. preuve d'enjeu

Définition
Mécanisme de validation de transactions qui repose sur la preuve de possession d'une quantité donnée de cryptomonnaie mise en garantie pour l'ajout d'un bloc à une chaîne de blocs.

Notes
Si une fraude est détectée dans le processus de validation des transactions, l'utilisateur désigné se verra confisquer la cryptomonnaie mise en garantie lors de la preuve d'enjeu.

preuve d'enjeu n. f.
preuve de participation n. f.
preuve d'intérêt n. f.

anglais
proof of stake
PoS

76. preuve d'enjeu déléguée

Définition

Mécanisme de validation de transactions qui repose sur la mise en garantie d'un montant de cryptomonnaie par des délégués élus parmi les utilisateurs d'une chaîne de blocs.

Notes

Ce mécanisme de validation prévoit que tout détenteur de jetons d'une cryptomonnaie peut voter pour des délégués en fonction du nombre de jetons qu'il détient (ex. : 1 jeton = 1 vote).

preuve d'enjeu déléguée n. f.
preuve de participation déléguée n. f.

anglais

delegated proof of stake
DPoS

---

77. prime de minage

Définition

Montant d'une cryptomonnaie remis à un mineur ou à un groupe de mineurs afin de le récompenser pour la création d'un nouveau bloc et d'encourager la participation au sein du réseau.

Notes

Selon le type de cryptomonnaie, la prime de minage peut être constituée par des jetons générés lors de la création du bloc ou par les frais des transactions associées à ce dernier.

La prime de minage constitue également, pour les cryptomonnaies dont le fonctionnement repose sur la preuve de travail, le moyen de mettre de nouveaux jetons en circulation.

prime de minage n. f.
récompense de minage n. f.
récompense de bloc n. f.

anglais

block reward

---

78. profondeur

Définition

Valeur relative attribuée à un bloc, qui correspond au nombre de blocs ayant été générés à sa suite dans une chaîne de blocs.

Notes
Chaque fois qu'un bloc est ajouté à une chaîne de blocs, la profondeur de tous les blocs le précédant augmente de un. La profondeur est un indicateur rapide du nombre de fois qu'un bloc a été validé depuis sa création, et donc de sa légitimité.

Il ne faut pas confondre la profondeur d'un bloc avec sa hauteur, celle-ci correspondant au nombre de blocs qui le précèdent.

profondeur n. f.
profondeur de bloc n. f.

anglais
block depth

---

79. racine de Merkle

Définition
Code de hachage terminal d'un arbre de Merkle, obtenu par la condensation d'un ensemble de blocs de données au moyen d'une fonction de hachage cryptographique.

Notes
Dans le domaine des chaînes de blocs, et plus précisément dans celui de la cryptomonnaie, la racine de Merkle générée à partir d'un bloc apparaît dans son en-tête, où elle agit à titre de signature numérique des transactions du bloc.

racine de Merkle n. f.

anglais
Merkle root

---

80. registre distribué

Définition
Registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entièreté du réseau et destinées à ne jamais être modifiées ou supprimées.

Notes
La mise à jour d'un registre distribué se répercute sur l'ensemble du réseau. Conséquemment, chaque membre possède en permanence la dernière version du registre.

registre distribué n. m.

anglais
distributed ledger
shared ledger

---

81. réseau de test

Définition
Réseau parallèle qui permet aux développeurs d'éprouver de nouvelles fonctionnalités ou de tester des mises à jour sans risquer de compromettre l'intégrité du réseau principal.

Notes
Lors du lancement d'une cryptomonnaie, le réseau de test fait également office de prototype que l'on peut montrer aux investisseurs afin de témoigner des avancées du projet.

réseau de test n. m.
réseau test n. m.

anglais
testnet
testing network

---

82. réseau principal

Définition
Réseau associé à un projet déployé sur une chaîne de blocs, qui permet le transfert de cryptomonnaie d'un expéditeur vers un destinataire, et dont l'objectif à terme est l'utilisation d'un service ou l'achat d'un produit.

Notes
Le réseau principal, en code source libre, est modifiable et peut donc évoluer.

réseau principal n. m.

anglais
mainnet
main network

---

83. seuil de hachage

Définition
Valeur définissant la difficulté du calcul nécessaire à la validation d'un bloc dans une chaîne de blocs recourant au mécanisme de validation par preuve de travail.

Notes
Le seuil de hachage varie en difficulté en fonction du nombre de zéros par lequel il débute.

Le seuil de hachage est ajusté périodiquement, notamment en fonction du temps de hachage moyen, du taux de hachage ainsi que de la cible de temps de hachage déterminée par un protocole de chaîne de blocs.

seuil de hachage n. m.

Le terme *seuil de hachage* a été proposé par l'Office québécois de la langue française en 2018 pour désigner ce concept.

anglais

target hash
target value
target difficulty
target

---

84. seuil minimal

Définition

Somme minimale qu'une équipe souhaite amasser lors d'une première émission de jetons afin de pouvoir mener à bien un projet.

Notes

En règle générale, le projet est abandonné lorsque le seuil minimal n'est pas atteint; les fonds sont alors rendus aux investisseurs.

seuil minimal n. m.
plancher d'investissement n. m.

Au pluriel, on écrira : *des seuils minimaux*, *des planchers d'investissement*.

anglais

soft cap

---

85. sommet sans précédent

Définition

Plus haut niveau jamais atteint par le cours des valeurs d'un marché, d'un secteur, d'un titre ou d'une cryptomonnaie.

sommet sans précédent n. m.
niveau record n. m.
haut sans précédent n. m.

anglais

all time high
ATH

---

86. stockage à chaud

Définition

Stockage d'une réserve de cryptomonnaie sur un support connecté à Internet, qui permet d'accéder rapidement aux fonds pour les transférer.

Notes

Il pourrait s'agir, par exemple, de stocker une clé privée dans un nuage informatique, sur une plateforme d'échange ou sur un téléphone intelligent.

On oppose généralement le stockage à chaud au stockage à froid, qui est moins risqué que le premier.

stockage à chaud n. m.

anglais

hot wallet

---

87. stockage à froid

Définition

Stockage d'une réserve de cryptomonnaie sur un support déconnecté d'Internet afin de réduire les risques de piratage, dont on se sert généralement pour les investissements à long terme.

Notes

Le stockage à froid peut être effectué en conservant la clé privée, qui donne accès à une somme, dans un document numérique, sur un ordinateur ou une clé USB, par exemple, ou simplement en inscrivant la clé sur une feuille.

stockage à froid n. m.
stockage hors ligne n. m.

Le terme *stockage à froid*, emprunté au domaine de l'alimentation, est employé de manière métaphorique et établit un parallèle avec la congélation des aliments pour leur conservation à long terme.

anglais

cold storage
cold wallet

---

88. taux de hachage

Définition

Indicateur permettant de mesurer la puissance de calcul d'un nœud ou d'un réseau utilisés pour la validation de transactions par preuve de travail.

Notes

Le taux de hachage s'exprime en nombre de calculs effectués par seconde ou de codes de hachage générés par seconde.

taux de hachage n. m.

anglais

hash rate

---

89. témoin séparé

Définition

Embranchement convergent ayant pour but de séparer les données de signature des blocs afin d'en augmenter la capacité de stockage.

Notes
L'utilisation de témoins séparés permet de favoriser l'extensibilité d'une chaîne de blocs.

témoin séparé n. m.

anglais
segregated witness
segwit

---

90. temps de hachage moyen

Définition
Moyenne du temps nécessaire à la création d'un nouveau bloc sur une chaîne de blocs.

Notes
Le temps de hachage moyen donne un aperçu du temps nécessaire à la validation d'une transaction sur une chaîne de blocs. Il dépend notamment du seuil de hachage et du taux de hachage de cette dernière.

temps de hachage moyen n. m.

Le terme *temps de hachage moyen* a été proposé par l'Office québécois de la langue française en 2018 pour désigner ce concept.

anglais
block time
average block time
block time length

---

91. vol de cryptomonnaie

Définition
Attaque informatique visant à dérober les jetons détenus par les utilisateurs d'une cryptomonnaie.

Notes
Pour effectuer un vol de cryptomonnaie, les pirates recourent à diverses stratégies, par exemple accéder par hameçonnage aux informations de connexion des utilisateurs, ou encore détourner les transferts de cryptomonnaie en remplaçant, au moyen d'un logiciel malveillant, l'identifiant du destinataire de la transaction. Ils peuvent également réaliser une attaque par majorité.

vol de cryptomonnaie n. m.
piratage de cryptomonnaie n. m.
cryptopiratage n. m.

anglais
cryptocurrency theft

---

92. zone de résistance

Définition

Zone de prix supérieure atteinte à plusieurs reprises par le cours d'une valeur, mais que cette dernière ne franchit pas en raison de la concentration de l'offre qu'elle engendre.

Notes

Il peut exister plusieurs zones de résistance selon la perspective adoptée par l'investisseur (court, moyen ou long terme).

Lorsque le cours d'une valeur finit par traverser une zone de résistance, cette dernière a souvent tendance à devenir une nouvelle zone de support.

zone de résistance n. f.
résistance n. f.

anglais

resistance
resistance level

---

93. zone de support

Définition

Zone de prix inférieure atteinte à plusieurs reprises par le cours d'une valeur, mais qu'elle ne franchit pas en raison de la concentration de la demande que cette situation engendre.

Notes

Il peut exister plusieurs zones de support selon la perspective adoptée par l'investisseur (court, moyen ou long terme).

Lorsque le cours d'une valeur finit par traverser une zone de support, cette dernière a souvent tendance à devenir une nouvelle zone de résistance.

zone de support n. f.
support n. m.

anglais

support
support level

VOCABULAIRE DE LA CRYPTOMONNAIE

Pour accéder à l'ensemble des vocabulaires de l'Office québécois de la langue française :
oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/index_lexvoc.html.

Pour connaître les outils et les services linguistiques de l'Office :
vitrinelinguistique.oqlf.gouv.qc.ca/a-propos-de-la-vitrine-linguistique/offre-de-services-linguistiques.

Pour consulter les ressources de la Vitrine linguistique :
vitrinelinguistique.oqlf.gouv.qc.ca.

Pour visiter le site de l'Office :
oqlf.gouv.qc.ca/accueil.aspx.

Office québécois de la langue française
Québec