Glossaire rapide

2022-03-04

# Glossaire rapide

Ce glossaire rapide contient de nombreux termes utilisés en relation avec le bitcoin. Ces termes sont utilisés tout au long du livre, alors mettez-les en signet pour une référence rapide.

adresse

Une adresse Bitcoin ressemble à 1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV. Il se compose d'une suite de lettres et de chiffres. Il s'agit en réalité d'une version codée en base58check d'un résultat de hachage à clé publique de 160 bits. Tout comme vous demandez aux autres d'envoyer un courriel à l’adresse de celle-ci, vous demanderez aux autres de vous envoyer des bitcoins à l'une de vos adresses Bitcoin.

bip

Bitcoin Improvement Proposals (ou Propositions d’améliorations du Bitcoin). Un ensemble de propositions que les membres de la communauté Bitcoin ont soumises pour améliorer Bitcoin. Par exemple, BIP-21 est une proposition visant à améliorer le schéma d'identificateur de ressource uniforme (URI) bitcoin.

bitcoin

Le nom de l'unité monétaire (unité de cryptomonnaie), du réseau et du logiciel.

bloc

Regroupement de transactions, marqué d'un horodatage et d'une empreinte digitale du bloc précédent. L'en-tête du bloc est haché (c.-à-d., on obtient un résultat de hachage) pour produire une preuve de travail, validant ainsi les transactions. Les blocs valides sont ajoutés à la chaîne de blocs principale par consensus du réseau.

blockchain (ou chaîne de blocs)

Une liste de blocs validés, chacun lié à son prédécesseur jusqu'au bloc de genèse.

récompense de bloc (alias récompense coinbase (ou unité de monnaie primaire du bloc)

Un montant inclus dans chaque nouveau bloc comme récompense par le réseau au mineur qui a trouvé la solution Proof-of-Work (ou Preuve de travail)). Environ tous les quatre ans, ou plus précisément tous les 210 000 blocs, la récompense de bloc globale est réduite de moitié. Il est actuellement de 6,25 BTC par bloc.

Byzantine Generals Problem (ou Problème des généraux Byzantins)

Un système informatique fiable doit pouvoir faire face à la défaillance d'un ou plusieurs de ses composants. Un composant défaillant peut présenter un type de comportement souvent négligé, à savoir l'envoi d'informations contradictoires à différentes parties du système. Le problème de faire face à ce type d'échec est exprimé abstraitement comme le Byzantine Generals Problem (ou Problème des généraux byzantins) (voir <https://fr.wikipedia.org/wiki/Probl%C3%A8me_des_g%C3%A9n%C3%A9raux_byzantins>).

bloc candidat

Un bloc qu'un mineur essaie toujours d'exploiter. Ce n'est pas encore un bloc valide, car il ne contient pas de Proof-of-Work (ou Preuve de travail) valide.

coinbase (ou unité de monnaie primaire du bloc) (alias données coinbase)

Un champ spécial utilisé comme seule entrée pour les transactions coinbase. Le champ de données coinbase permet de réclamer la récompense de bloc et fournit jusqu'à 100 octets pour les données arbitraires. À ne pas confondre avec la "transaction coinbase" ou la "récompense coinbase".

transaction coinbase

La première transaction d'un bloc; toujours créé par un mineur. Le coinbase est unique dans le bloc. À ne pas confondre avec coinbase (données coinbase) ou "récompense coinbase".

stockage à froid

Fait référence à la conservation d'une réserve de bitcoins hors ligne. Le stockage à froid est réalisé lorsque les clés privées bitcoin sont créées et stockées dans un environnement hors ligne sécurisé. Le stockage à froid est important pour quiconque possède des avoirs en bitcoins. Les ordinateurs en ligne sont vulnérables aux pirates et ne doivent pas être utilisés pour stocker une quantité importante de bitcoins. (note du traducteur: l’auteur est un peu paranoïde; les noeuds sont en ligne. Si les noeuds sont insécures, c’est la fin de ce système et de ce livre.) ;)

confirmations

Une fois qu'une transaction est incluse dans un bloc, elle a une confirmation. Dès qu'un autre bloc est miné sur la même chaîne de blocs, la transaction a deux confirmations, et ainsi de suite. Six confirmations ou plus sont considérées comme une preuve suffisante qu'une transaction ne peut pas être annulée.

consensus

Lorsque plusieurs nœuds, généralement la plupart des nœuds du réseau, ont tous les mêmes blocs dans leur meilleure chaîne de blocs validée localement. À ne pas confondre avec les règles de consensus.

règles de consensus

Les règles de validation de bloc que les nœuds complets suivent pour rester en consensus avec les autres nœuds. A ne pas confondre avec le consensus.

difficulté

Un paramètre à l'échelle du réseau qui contrôle la quantité de calculs nécessaires pour produire une preuve de travail (ou le Proof-of-Work).

reciblage de difficulté

Un recalcul à l'échelle du réseau de la difficulté qui se produit une fois tous les 2 016 blocs et prend en compte la puissance de hachage des 2 016 blocs précédents.

cible de difficulté

Une difficulté pour le calcul dans tout le réseau et qui permet de solutionner et valider l’ajout d’un bloc environ toutes les 10 minutes.

double dépense

La double dépense est le résultat d'avoir réussi à dépenser de l'argent plus d'une fois. Bitcoin protège contre les doubles dépenses en vérifiant chaque transaction ajoutée à la chaîne de blocs pour s'assurer que les entrées de la transaction n'avaient pas déjà été dépensées auparavant.

ECDSA

Elliptic Curve Digital Signature Algorithm ou ECDSA est un algorithme cryptographique utilisé par bitcoin pour garantir que les fonds ne peuvent être dépensés que par leurs propriétaires légitimes.

nombre aléatoire explicite supplémentaire

Au fur et à mesure que la difficulté augmentait, les mineurs parcouraient souvent les 4 milliards de nombres aléatoires explicites (nonce) sans trouver de bloc. Étant donné que le script coinbase peut stocker entre 2 et 100 octets de données, les mineurs ont commencé à utiliser cet espace comme espace pour un nombre aléatoire explicite supplémentaire, leur permettant d'explorer une gamme beaucoup plus large de valeurs d'en-tête de bloc pour trouver des blocs valides.

frais

L'expéditeur d'une transaction inclut souvent une valeur de frais au réseau pour le traitement de la transaction demandée. La plupart des transactions nécessitent des frais minimum de 0,5 mBTC.

fourche

La fourche, également connue sous le nom de fourche accidentelle, se produit lorsque deux blocs ou plus ont la même hauteur de bloc, forçant la chaîne de blocs à se dédoubler. Cela se produit généralement lorsque deux mineurs ou plus trouvent des blocs presque en même temps. Peut également se produire dans le cadre d'une attaque.

bloc de genèse

Le premier bloc de la chaîne de blocs, utilisé pour initialiser la cryptomonnaie (ou cybermonnaie).

halving (ou réduction de moitié)

Un événement de réduction de moitié se produit lorsque la récompense de bloc est réduite de moitié, ce qui se produit environ tous les quatre ans (ou précisément tous les 210 000 blocs). Bitcoin a déjà connu trois événements de réduction de moitié : en 2012 (de 50 à 25 BTC), en 2016 (de 25 à 12,5 BTC) et en 2020 (de 12,5 à 6,25 BTC).

fourche dure

La fourche dure, également connu sous le nom de Hard-Forking Change, est une divergence permanente dans la chaîne de blocs, se produit généralement lorsque les nœuds non mis à niveau ne peuvent pas valider les blocs créés par les nœuds mis à niveau qui suivent les nouvelles règles de consensus. À ne pas confondre avec une fourche, une fourche molle, une fourche de code ou une fourche Git, mais tout de même un nouvel embranchement d’une arborescence de données (avec une source parent unique).

portefeuille matériel (hardware)

Un portefeuille matériel est un type spécial de portefeuille bitcoin qui stocke les clés privées de l'utilisateur dans un périphérique matériel sécurisé.

résultat de hachage

Une empreinte numérique d'une entrée binaire.

hashlocks (ou serrure par empreinte numérique)

Un hashlock (ou serrure par empreinte numérique) est un type de contrainte qui limite les dépenses d'une sortie jusqu'à ce qu'une donnée spécifique soit révélée publiquement. Les hashlocks ont la propriété utile qu'une fois qu'un hashlock est ouvert publiquement, tout autre hashlock sécurisé à l'aide de la même clé peut également être ouvert. Cela permet de créer plusieurs sorties qui sont toutes encombrées par le même hashlock et qui deviennent toutes dépensables en même temps.

Protocole HD

Le protocole de création et de transfert de clés Hierarchical Deterministic (HD) (BIP-32), qui permet de créer des clés enfants à partir de clés parents dans une hiérarchie.

Portefeuille HD

Portefeuilles utilisant le protocole de création et de transfert de clés Hierarchical Deterministic (HD Protocol) (BIP-32).

Portefeuille d’amorçage HD

Le portefeuille d’amorçage HD ou la valeur d’amorçage est une valeur potentiellement courte utilisée comme valeur racine pour générer la clé privée principale et le code de chaîne principal pour un portefeuille HD.

HTLC

Un contrat Hashed TimeLock ou HTLC est une classe de paiements qui utilisent des hashlocks (ou serrures par empreintes numériques) et des timelocks (ou serrures par horodatage) pour exiger que le destinataire d'un paiement reconnaisse avoir reçu le paiement avant une date limite en générant une preuve cryptographique de paiement ou renonce à la possibilité de réclamer le paiement, le retournant au payeur.

KYC

Know Your Customer (ou Connaître son client) (KYC) est le processus d'une entreprise qui identifie et vérifie l'identité de ses clients. Le terme est également utilisé pour désigner la réglementation bancaire qui régit ces activités.

LevelDB

LevelDB est un moyen de stockage clé-valeur open source sur disque. LevelDB est une bibliothèque légère à usage unique pour la persistance avec des liaisons sur de nombreuses plates-formes.

Lightning Networks

Lightning Network est une implémentation de Hashed Timelock Contracts (HTLC) avec des canaux de paiement bidirectionnels qui permettent aux paiements d'être acheminés en toute sécurité sur plusieurs canaux de paiement pair à pair. Cela permet la formation d'un réseau où n'importe quel pair sur le réseau peut payer n'importe quel autre pair même s'ils n'ont pas directement de canal ouvert entre eux.

Locktime (ou valeur de relâche de transaction)

Locktime, ou plus techniquement nLockTime, est la partie d'une transaction qui indique la première heure où le premier bloc auquel cette transaction peut être ajoutée à la chaîne de blocs. C’est une valeur horodatée servant de date ultérieur pour une transaction; comme un chèque postdaté.

mempool

Le bitcoin Mempool (bassin de mémoire) est une collection de toutes les données de transaction dans un bloc qui ont été vérifiées par les nœuds Bitcoin, mais qui ne sont pas encore confirmées.

racine de merkle

Le nœud racine d'un arbre Merkle, un descendant de toutes les paires hachées de l'arbre. Les en-têtes de bloc doivent inclure une racine merkle valide issue de toutes les transactions de ce bloc.

arbre de merkle

Un arbre construit en hachant des données appariées (les feuilles), puis en appariant et en hachant les résultats jusqu'à ce qu'il ne reste qu'un seul résultat de hachage, la racine de Merkle. En bitcoin, les feuilles sont presque toujours des transactions d'un seul bloc.

mineur

Un nœud de réseau qui trouve une preuve de travail valide pour les nouveaux blocs, par hachage répété.

récompense minière

Les récompense que les mineurs reçoivent en échange de la sécurité fournie par l'exploitation minière, comprend les nouvelles pièces bitcoin créées avec chaque nouveau bloc, également appelées récompense de bloc ou récompense coinbase, et les frais de transaction de toutes les transactions incluses dans le bloc.

multisignature

La multisignature (multisig) fait référence à l'exigence d'un nombre minimum (M) de clés (N) pour autoriser une transaction M-sur-N.

réseau

Un réseau pair à pair qui propage les transactions et les bloques à chaque nœud Bitcoin du réseau.

nonce (ou nombre aléatoire explicite)

Le "nonce" (ou nombre aléatoire explicite) dans un bloc bitcoin est un champ de 32 bits (4 octets) dont la valeur est définie de manière à ce que le résultat de hachage du bloc contienne une série de zéros non significatifs. Les autres champs ne peuvent pas être modifiés, car ils ont une signification définie.

transactions hors chaîne

Une transaction hors chaîne est le mouvement de valeur en dehors de la chaîne de blocs, alors qu'une transaction en chaîne&#x2014 est simplement appelée *une transaction*&#x2014. La transaction hors chaîne modifie la chaîne de blocs et dépend de cette dernière pour déterminer sa validité. Une transaction hors chaîne de blocs s'appuie sur d'autres méthodes pour enregistrer et valider la transaction.

opcode

Codes d'opération du langage de script bitcoin qui poussent des données ou exécutent des fonctions dans un script pubkey ou un script de signature.

Protocole Open Assets (ou Actifs ouverts)

Le protocole Open Assets (ou Actifs ouverts) est un protocole simple et puissant construit au-dessus de la chaîne de blocs Bitcoin. Il permet l'émission et le transfert d'actifs créés par l'utilisateur.

OP\_RETURN

Un opcode (ou code d’opération) utilisé dans l'une des sorties d'une transaction OP\_RETURN. A ne pas confondre avec la transaction OP\_RETURN.

Transaction OP\_RETURN

Un type de transaction qui ajoute des données arbitraires à un script pubkey prouvé que les nœuds complets n'ont pas à stocker dans leur base de données UTXO. A ne pas confondre avec l'opcode OP\_RETURN.

bloc orphelin

Les blocs dont le bloc parent n'a pas été traité par le nœud local, ils ne peuvent donc pas encore être entièrement validés. À ne pas confondre avec le bloc obsolète.

orphan transactions

Transactions qui ne peuvent pas entrer dans le bassin de mémoire (Mempool) en raison d'une ou plusieurs transactions d'entrée manquantes.

extrant

L’Output (le produit sorti ou l’extrant), la sortie de transaction ou TxOut est une sortie dans une transaction qui contient deux champs : un champ de valeur pour transférer zéro ou plusieurs satoshis et un script pubkey pour indiquer quelles conditions doivent être remplies pour que ces satoshis soient dépensés davantage.

P2PKH

Les transactions qui paient une adresse Bitcoin contiennent des scripts P2PKH ou Pay To PubKey Hash. Une sortie verrouillée par un script P2PKH peut être déverrouillée (dépensée) en présentant une clé publique et une signature numérique créée par la clé privée correspondante.

P2SH

P2SH ou Pay-to-Script-Hash est un nouveau type de transaction puissant qui simplifie grandement l'utilisation de scripts de transaction complexes. Avec P2SH le script complexe qui détaille les conditions de dépense de la sortie (redeem script) n'est pas présenté dans le script de verrouillage. Au lieu de cela, seul un résultat de hachage de celui-ci se trouve dans le script de verrouillage.

Adresse P2SH

Les adresses P2SH sont des encodages Base58Check du résultat de hachage de 20 octets d'un script. Ils utilisent le préfixe de version "5", ce qui donne des adresses encodées en Base58Check qui commencent par un "3". Les adresses P2SH cachent toute la complexité, de sorte que la personne effectuant un paiement ne voit pas le script.

P2WPKH

La signature d'un P2WPKH (Pay-to-Witness-Public-Key-Hash) contient les mêmes informations qu'une dépense P2PKH, mais se trouve dans le champ témoin au lieu du champ scriptSig. Le scriptPubKey est également modifié.

P2WSH

La différence entre P2SH et P2WSH (Pay-to-Witness-Script-Hash) concerne le changement d'emplacement de la preuve cryptographique du champ scriptSig au champ témoin et le scriptPubKey qui est également modifié.

portefeuille papier

Dans le sens le plus spécifique, un portefeuille papier est un document contenant toutes les données nécessaires pour générer un nombre quelconque de clés privées bitcoin, formant un portefeuille de clés. Cependant, les gens utilisent souvent le terme pour désigner tout moyen de stocker des bitcoins hors ligne en tant que document physique. Cette deuxième définition comprend également les clés papier et les codes échangeables.

phrase de passe

Une phrase de passe est une chaîne de caractères facultative créée par l'utilisateur qui sert de facteur de sécurité supplémentaire protégeant la valeur d’amorçage, même lorsque la valeur d’amorçage est compromise par un voleur. Il peut également être utilisé comme une forme de pot de miel, où une phrase de passe choisie (une adresse bitcoin, un URL ou autre) mène à un portefeuille avec une petite quantité de fonds utilisée pour distraire un attaquant du "vrai" portefeuille qui contient la majorité des fonds.

canaux de paiement

Un canal de micropaiement ou canal de paiement est une classe de techniques conçues pour permettre aux utilisateurs d'effectuer plusieurs transactions bitcoin sans engager toutes les transactions dans la chaîne de blocs Bitcoin. Dans un canal de paiement typique, seules deux transactions sont ajoutées à la chaîne de blocs, mais un nombre illimité ou presque illimité de paiements peut être effectué entre les participants.

exploitation minière groupée

L'exploitation minière en groupe est une approche d'exploitation minière dans laquelle plusieurs clients générateurs contribuent à la génération d'un bloc, puis divisent la récompense du bloc en fonction de la puissance de traitement apportée.

Proof-of-Stake (ou Preuve d’enjeu)

La preuve d’enjeu (PoS) est une méthode par laquelle un réseau de chaîne de blocs de cryptomonnaie vise à atteindre un consensus distribué. La preuve d’enjeu demande aux utilisateurs de prouver qu'ils sont propriétaires d'un certain montant de devise (leur « enjeu » ou « participation » dans la devise).

Proof-of-Work (ou Preuve de travail)

Une donnée qui nécessite des calculs importants pour être trouvée. Dans le bitcoin, les mineurs doivent trouver une solution numérique à l'algorithme SHA256 qui répond à une cible à l'échelle du réseau, la cible de difficulté.

RIPEMD-160

RIPEMD-160 est une fonction de hachage cryptographique 160 bits. RIPEMD-160 est une version renforcée de RIPEMD avec un résultat de hachage de 160 bits, et devrait être sécurisé pour les dix prochaines années ou plus.

satoshi

Un satoshi est la plus petite dénomination de bitcoin pouvant être enregistrée sur la blockchain. Il équivaut à 0,00000001 bitcoin et porte le nom du créateur du bitcoin, Satoshi Nakamoto.

Satoshi Nakamoto

Satoshi Nakamoto est le nom utilisé par la ou les personnes qui ont conçu le bitcoin et créé son implémentation de référence originale, Bitcoin Core. Dans le cadre de la mise en œuvre, ils ont également conçu la première base de données chaîne de blocs. Dans le processus, ils ont été les premiers à résoudre le problème de la double dépense pour la monnaie numérique. Leur véritable identité reste inconnue.

Script

Bitcoin utilise un système de script pour les transactions. Comme Forth, Script est simple, basé sur une pile et traité de gauche à droite. Il n'est délibérément pas complet de Turing et sans boucles.

ScriptPubKey (alias script pubkey): : ScriptPubKey ou script pubkey, est un script inclus dans les sorties qui définit les conditions qui doivent être remplies pour que ces satoshis soient dépensés. Les données permettant de remplir les conditions peuvent être fournies dans un script de signature.

ScriptSig (ou Script de signature): : ScriptSig ou script de signature, sont les données générées par un dépensier qui sont presque toujours utilisées comme variables pour satisfaire un script pubkey.

clé secrète (ou clé privée): : Le numéro secret qui déverrouille le bitcoin envoyé à l'adresse correspondante. Une clé secrète ressemble à ceci :

+

5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh

Témoin Séparé

Le témoin séparé est une mise à niveau du protocole Bitcoin dans laquelle les données de signature ("témoin") sont séparées des données de l'expéditeur/destinataire pour optimiser davantage la structure des transactions. Le témoin Séparé a été implémenté comme un embranchement convergent ; un changement qui rend techniquement les règles du protocole de bitcoin plus restrictives.

SHA

Le Secure Hash Algorithm ou SHA est une famille de fonctions de hachage cryptographiques publiées par le National Institute of Standards and Technology (NIST).

Simplified Payment Verification (SPV ou Vérification simplifiée des paiements): : SPV ou vérification simplifiée des paiements est une méthode permettant de vérifier que des transactions particulières ont été incluses dans un bloc, sans télécharger le bloc entier. Cette méthode de vérification est souvent utilisée par les clients Bitcoin légers.

embranchement convergent

L’embranchement convergent ou le Soft-Forking Change est un fourche temporaire dans la chaîne de blocs qui se produit généralement lorsque les mineurs utilisant des nœuds non mis à niveau ne suivent pas une nouvelle règle de consensus que leurs nœuds ne connaissent pas. À ne pas confondre avec fourche, fourche dure, fourche logicielle ou fourche de Git.

bloc périmé

Un bloc valide qui a été extrait avec succès mais qui n'est pas inclus dans la branche principale actuelle (avec la plupart des preuves de travail cumulatives), car un autre bloc valide qui a été extrait à la même hauteur a vu sa chaîne étendue en premier. Le mineur d'un bloc périmé ne reçoit pas la récompense du bloc ni les frais de transaction de ce bloc. À ne pas confondre avec le bloc orphelin ou le bloc candidat.

timelocks (ou serrures horaires)

Un timelock (ou serrure horaire) est un type de contrainte qui limite la dépense de certains bitcoins jusqu'à une heure future ou une hauteur de bloc spécifiée. Les timelocks figurent en bonne place dans de nombreux contrats bitcoin, y compris les canaux de paiement et les contrats de timelock hachés.

transaction

En termes simples, un transfert de bitcoin d'une adresse à une autre. Plus précisément, une transaction est une structure de données signée exprimant un transfert de valeur. Les transactions sont transmises sur le réseau Bitcoin, collectées par les mineurs et incluses dans des blocs, rendus permanents sur la chaîne de blocs.

bassin de transactions

Une collection non ordonnée de transactions qui ne sont pas en blocs dans la chaîne principale, mais pour lesquelles nous avons des transactions d'entrée.

Complétude de Turing

Un langage de programmation est appelé "Turing complet" s'il peut exécuter n'importe quel programme qu'une machine de Turing peut exécuter, avec suffisamment de temps et de mémoire.

unspent transaction output (UTXO ou sortie de transaction non dépensée)

UTXO est une sortie de transaction non dépensée qui peut être dépensée comme entrée dans une nouvelle transaction.

portefeuille

Logiciel qui contient toutes vos adresses Bitcoin et clés secrètes. Utilisez-le pour envoyer, recevoir et stocker vos bitcoins.

Wallet Import Format (WIF ou Format d’importation de portefeuille)

WIF ou Wallet Import Format (format d’importation de portefeuille) est un format d'échange de données conçu pour permettre l'exportation et l'importation d'une seule clé privée avec un indicateur indiquant s'il utilise ou non une clé publique compressée.

Certaines définitions fournies ont été extraites sous une licence CC-BY de [bitcoin Wiki](https://en.bitcoin.it/wiki/Main_Page) ou d'autres documentations à source libre.