asprom

Glossaire Cryptomonnaie
Lexique du monde des cryptomonnaies et de la blockchain

Adresse

Une adresse publique est une série de caractères alphanumériques (0x123…f4) qui identifie de manière unique un compte de cryptomonnaie. C'est l'adresse que vous donnez à quelqu'un pour recevoir des fonds, semblable à votre RIB dans le système bancaire. La détenir ne permet donc pas d'envoyer des fonds, cette dernière ayant vocation à être partagée.
L'adresse privée, en revanche, est une chaîne de caractères alphanumériques qui permet d'accéder à un compte de cryptomonnaies et de signer des transactions. Cette adresse ne doit jamais être partagée avec quiconque, car toute personne ayant accès à l'adresse privée peut accéder et transférer les fonds liés à cette adresse.

En d'autres termes, l'adresse publique est comme votre adresse postale, elle peut être partagée pour recevoir des fonds, mais l'adresse privée est comme votre clé de maison, elle ne doit jamais être partagée car elle permet d'accéder à l'intégralité des actifs qui se trouve sur le compte.
Une adresse correspond à une clé publique qui permet de recevoir des crypto-monnaies ou d'en envoyer. Cette clé publique peut prendre la forme d'une suite de lettres et de chiffres ou d'un QR code. On pourrait comparer cette adresse à un RIB/IBAN pour les monnaies classiques ou à une adresse email pour l'envoi de mails.

Airdrop

Un Airdrop se produit lorsqu'une équipe souhaite promouvoir le lancement d'une nouvelle crypto-monnaie. Ils vont alors offrir des tokens de façon périodique et contrôlée à des personnes qui remplissent un ensemble spécifique de caractéristiques (exemple : être un membre actif sur un forum et mettre dans sa signature le lien du site Internet de la crypto-monnaie en question).

Algorithme de consensus

Un algorithme de consensus est une méthode par laquelle les différents nœuds d'un réseau décentralisé s'accordent sur un état unique et cohérent pour le réseau. Dans le contexte des blockchains et des cryptomonnaies, les algorithmes de consensus sont essentiels pour assurer l'intégrité et la sécurité des données stockées sur le réseau, tout en évitant les doubles dépenses et autres problèmes de sécurité.
Il existe plusieurs types d'algorithmes de consensus, chacun ayant ses avantages et ses inconvénients. Les principaux types d'algorithmes de consensus utilisés dans les blockchains utilisent la preuve de travail (PoW) ou la preuve d'enjeu (PoS) :

All-in

Investir tous les fonds que l'on possède sur une même crypto-monnaie à un instant T (généralement une très mauvaise idée).

Altcoin / Monnaie Alternative

Altcoin est l'abréviation pour « Alternative Coin ». Un altcoin désigne toutes les crypto-monnaies autres que le Bitcoin
Altcoin est un terme qui se réfère à toutes les cryptomonnaies qui ont été créées après le bitcoin, la toute première cryptomonnaie à avoir été lancée en 2009. Le terme « altcoin » est une combinaison de deux mots, « alt » qui signifie alternatif et « coin » qui fait référence aux pièces de monnaie. Les altcoins sont donc des alternatives à Bitcoin, mais ils partagent souvent des points communs avec ce dernier.
Les altcoins sont également basés sur la technologie de la blockchain, mais ils peuvent différer considérablement de Bitcoin en termes de protocoles, d'algorithmes de consensus et de fonctionnalités.
Il existe aujourd'hui des milliers d'altcoins différents, chacun ayant ses propres caractéristiques et fonctionnalités.
Tout comme le bitcoin, le cours des altcoins est hautement volatil et peut subir des fluctuations de valeur importantes en très peu de temps. De plus, comme ils sont souvent moins liquides que les bitcoins, leur achat et leur vente peuvent être plus difficiles. Les investisseurs doivent donc être conscients de ces risques avant d'investir dans les altcoins.

Altcoin season

Altcoin season est un terme couramment utilisé dans l'industrie des cryptomonnaies pour décrire une période de temps où les cours de la plupart des altcoins sont en hausse simultanément, plutôt que de manière individuelle et isolée, et affichent des performances supérieures à celles du bitcoin.
Il s'agit souvent d'une période de forte volatilité et de fluctuations rapides des prix, où les altcoins peuvent connaître des hausses de prix importantes en très peu de temps.
Si elles suivent souvent une période de hausse du prix du bitcoin, les périodes d'altcoin season peuvent être imprévisibles et de durées variables. Elles s'étalent généralement sur quelques jours à quelques semaines, voire quelques mois. Les facteurs déclenchant peuvent être de différentes natures : développements technologiques, annonces de partenariats ou de collaborations, entrée de nouveaux investisseurs sur le marché, géopolitique, changement de législation…
Toutefois, l'altcoin season ne garantit pas des performances à long terme. Une fois qu'elle est terminée, les prix peuvent baisser rapidement, en particulier si ces derniers sont surestimés et que les altcoins n'ont pas de fondamentaux solides pour soutenir leur croissance.

AMA Ask Me Anything

Un Ask-Me-Anything (AMA), en français « demandez-moi n'importe quoi » désigne une session de questions-réponses où les utilisateurs posent des questions en direct à un invité (ou un groupe) qui répond en temps réel.
En effet, les AMA sont généralement organisées par des développeurs de projets autour de la blockchain et des cryptomonnaies, des projets NFT ou des investisseurs, bien qu'ils puissent se faire à l'initiative de n'importe qui. Les AMA sont généralement annoncées à l'avance sur les réseaux sociaux, ce qui permet aux participants d'en prendre connaissance et de préparer leurs questions

AMF

L’AMF est l’acronyme de « Autorité des Marchés Financiers« . Il s’agit d’une autorité administrative indépendante créée en 2003 en France, chargée de la régulation et du contrôle des marchés financiers.
L’AMF a pour mission principale de protéger les épargnants en veillant au bon fonctionnement des marchés financiers et en assurant la transparence de l’information financière. Elle est également chargée de superviser et de réguler les professionnels de la finance, tels que les établissements de crédit, les intermédiaires financiers, les sociétés de gestion d’actifs ou encore les entreprises d’investissement.
Elle est ainsi habilitée à exercer différents pouvoirs tels que la délivrance d’agréments pour les professionnels de la finance, la surveillance des activités des établissements financiers, la régulation des marchés, la surveillance des transactions et l’investigation en cas de fraudes ou de manipulations de marché.
Concernant les cryptomonnaies, l’AMF a mis en place un régime d’agrément pour les Prestataires de Services sur Actifs Numériques (PSAN) depuis 2019. Cet agrément est délivré sous réserve du respect d’un certain nombre de critères, notamment en matière de gouvernance, de sécurité des systèmes d’information, de lutte contre le blanchiment d’argent et le financement du terrorisme, ainsi que de protection des investisseurs. Les PSAN agréés par l’AMF peuvent proposer des services tels que l’achat, la vente et la conservation de cryptomonnaies pour le compte de tiers, ainsi que des prestations de conseil en investissement sur ces actifs.

AML (Anti-Money Laundering) ou Anti Blanchiment d'Argent

Les mesures AML découlent souvent des règlementations d'un état et ont pour but de prévenir le risque de convertir des fonds qui auraient été obtenus illégalement.

APR

L'APR (Annual Percentage Rate) est l'abréviation de « Taux Annuel en Pourcentage ». Ce terme correspond au taux de rendement annuel d'un investissement, sans prendre en compte les intérêts composés.

APY

L'APY(Annuel Percentage Yield) est l'abréviation de « Rendement Annuel en Pourcentage ». Ce terme correspond au rendement annuel d'un investissement en prenant en compte l'effet des intérêts composés.

Arbitrage

Activité consistant à tirer du profit de la différence de prix qu'il peut y avoir entre plusieurs exchanges pour acheter sur l'un et revendre sur l'autre.

Arbre de Merkle

Un arbre de Merkle, également connu sous le nom d’arbre de hachage binaire, est une structure de données utilisée dans les technologies de blockchain et de cryptographie pour vérifier et valider efficacement les données contenues dans les ensembles de données

volumineux. Les arbres de Merkle tirent leur nom de Ralph Merkle, un cryptographe et informaticien américain qui a inventé cette structure de données en 1979.
L'arbre de Merkle est une structure d'arbre binaire où chaque nœud de l'arbre est le résultat d'une fonction de hachage appliquée aux données des nœuds enfants. Les nœuds feuilles (nœuds sans enfants) sont créés en appliquant une fonction de hachage aux données réelles, tandis que les nœuds internes sont créés en hachant les valeurs de hachage de leurs nœuds enfants. Ce processus est répété jusqu'à ce qu'il ne reste qu'un seul nœud, appelé racine de l'arbre de Merkle ou simplement racine de Merkle.

ASIC (Application Specific Integrated Circuit)

Ce sigle signifie **A**pplication **S**pecific **I**ntegrated **C**ircuit, ce sont des machines dédiées à une tâche unique. Dans le cadre des cryptos-monnaies, les ASICs servent à résoudre un algorithme de minage comme le SHA-256. Pour être plus précis, ce sont des équations contenues dans l'algorithme qui sont résolues.

Ask

Prix auquel les vendeurs souhaitent vendre une crypto-monnaie donnée

ATH (All Time High) / ATL (All Time Low)

ATH : prix le plus haut jamais atteint par une crypto-monnaie
ATL : prix le plus bas jamais atteint par une crypto-monnaie

Atomic Swaps

Les atomic swaps permettent à deux actifs situés sur des blockchains différentes d'être échangés entre eux, sans intermédiaire.

Ava Labs

Ava Labs est une société dont l'objectif est de simplifier le déploiement de solutions Web3, basées sur la plateforme de blockchain open-source Avalanche. Crée en 2018 par trois chercheurs de l'université Cornell, Ava Labs vise à résoudre certains des problèmes rencontrés par les autres blockchains en fournissant une plateforme rapide, évolutive et interopérabl

Bandes de Bollinger

Les bandes de Bollinger forment un indicateur technique utilisé pour mesurer la volatilité des prix d'un actif financier. Créé par le trader et analyste John Bollinger dans les années 1980, il est basé sur une moyenne mobile simple (SMA) ainsi que sur deux bandes, une supérieure et une inférieure, qui sont établies en fonction de l'écart-type des prix de l'actif.

Bear Market

Marché à tendance baissière.

Bid

Prix auquel les acheteurs souhaitent acheter une crypto-monnaie donnée

Binance

Binance est la plus grande plateforme d'échange de cryptomonnaies au monde. Créée en 2017, en réponse à l'explosion de la demande pour les cryptomonnaies et les plateformes d'échange qui permettent de les acheter et de les vendre. La société a été fondée par Changpeng Zhao, un entrepreneur ayant travaillé précédemment pour Bloomberg Tradebook

Binance Coin (BNB)

Le Binance Coin, ou BNB, est une cryptomonnaie créée en 2017 dans le cadre d'une ICO permettant à la plateforme d'échange de cryptomonnaies Binance de lever des fonds pour accélérer son développement. Binance est l'une des plateformes d'échange de cryptomonnaies les plus populaires au monde, avec un volume de transactions quotidien élevé et une gamme de produits et services très large.

BIP (Bitcoin Improvement Proposal)

Le BIP est un document conçu pour présenter de nouvelles caractéristiques ou informations au réseau Bitcoin. C'est la façon standard pour échanger des informations, car le réseau Bitcoin n'a aucune structure formelle, les propositions sont soumises par la communauté et sont approuvées par celle-ci.

Bitcoin

Le Bitcoin est une monnaie électronique décentralisée conçue en 2009 par un développeur non identifié utilisant le pseudonyme de Satoshi Nakamoto. Quand on l'écrit **B**itcoin, il s'agit du protocole ou réseau. Quand on l'écrit **b**itcoin, il s'agit de la crypto-monnaie.
Symbole monétaire officiel : ₿
Sigles utilisés par les plateformes d'échanges : BTC et XBT

Bitcoin ATM

ATM est l'acronyme anglais pour DAB (Distributeur Automatique de Billets). Un ATM Bitcoin vous permet d'acheter des bitcoins avec des billets de banque et parfois de retirer vos bitcoins contre des billets de banque.

BitPay

BitPay est un système de paiement pour bitcoins qui permet aux commerçants d'accepter les paiements en bitcoins. Il s'agit d'un moyen de démocratisation du Bitcoin.

Bittrex

Bittrex est une plateforme d'échange de cryptomonnaies créée en 2014 par 3 ingénieurs en cybersécurité : Bill Shihara, Richie Lai, Rami Kawach et Ryan Hentz. Le siège social de

l’entreprise se situe à Seattle, aux États-Unis. La plateforme est accessible via le site internet ou à l’aide d’une application mobile dédiée.
Bittrex propose une large gamme de cryptomonnaies, dont les principales, telles que BTC, ETH, ou encore LTC, ainsi que de nombreuses autres cryptomonnaies moins connues. La plateforme propose également une interface utilisateur conviviale et des outils de trading avancés pour les traders professionnels.

Bloc

Un bloc est une sorte de fichier contenant toutes les transactions précédents sa création. Une fois le bloc "remplis", il est "scellé" et rattaché aux anciens blocs afin de former une chaîne (la blockchain). Un nouveau bloc est créé, il contiendra les transactions en cours. Pour le Bitcoin, un bloc est créé toutes les 10 minutes environ.

Bloc Genesis (Block Genesis)

Premier bloc d'une blockchain.

Récompense de Bloc (Block Reward)

Récompense reversée par la Blockchain lorsqu'un bloc est trouvé. Contrairement à ce que l'on pourrait croire, trouver un bloc n'apporte pas une unité de la crypto en récompense, mais une valeur qui est initialement fixée par les développeurs de la crypto et ajustée dans le temps. Pour le Bitcoin par exemple, cette valeur est actuellement de 12,5 bitcoins par bloc et sera divisée par 2 lors du halving du Bitcoin en 2020. Elle passera donc à 6,25 bitcoins par bloc, jusqu'au prochain halving.

Blockchain / Chaîne de Blocs

La blockchain est une liste complète de tous les blocs de transactions complétés depuis le début du Bitcoin. Afin de renforcer la sécurité du système, la blockchain a été conçue de sorte que chaque bloc de transactions contienne le hash produit à partir du bloc précédent. La blockchain est une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente, et fonctionnant sans organe central de contrôle. Par extension, la blockchain désigne une base de données sécurisée et distribuée (car partagée par ses différents utilisateurs), contenant un ensemble de transactions dont chacun peut vérifier la validité. La blockchain peut donc être comparée à un grand livre comptable public, anonyme et infalsifiable.

Bottom / Creux

Le bottom (creux en français) est le prix le plus bas qu’un actif atteindra avant de repartir à la hausse. Il s’oppose au top (sommet).

Bulle spéculative

Une bulle spéculative se produit lorsque le prix d’un actif (ou d’une classe d’actif) augmente de manière excessive et rapide, souvent en raison d’une demande très importante de la part des investisseurs, sans justification provenant de sa valeur fondamentale.

Les bulles spéculatives se produisent souvent dans les secteurs en pleine croissance, tels que les technologies de pointe (internet, les cryptomonnaies), ou dans les secteurs où la demande est forte, tels que l'immobilier. Les investisseurs spéculatifs cherchent alors à acheter des actifs en espérant les revendre à un prix plus élevé dans le futur. Cependant, cette demande excessive entraîne souvent une augmentation artificielle des prix, qui ne reflète pas la valeur réelle des actifs.

Bullish

« Bullish » est un terme utilisé sur les marchés financiers pour décrire une tendance positive caractérisée par une anticipation d'une hausse des prix à court ou moyen terme. Les investisseurs « bullish » sont optimistes quant à la valeur future des actifs et cherchent souvent à acheter des actifs dans l'espoir d'une augmentation de leur valeur.

Bull Market

Marché à tendance haussière. On parle également de Bullish pour qualifier cette situation.

Burn

Le fait de détruire des tokens d'une crypto-monnaie.

CEX

Acronyme de « Centralized EXchange », les plateformes d'échange de cryptomonnaies centralisées. Un CEX met en relation acheteurs et vendeurs par l'intermédiaire d'un carnet d'ordres et procède à la vérification d'identité de ses utilisateurs. Les frais y sont bien plus faibles qu'avec les DEX, puisque les CEX sont centralisés et que tous les échanges se passent en interne et non sur la blockchain.

CBDC / Monnaie numérique de banque centrale

Les *central bank digital currencies* (CBDC), ou monnaies numériques de banque centrale (MNBC), sont des projets d'actifs numériques émis au niveau étatique par les banques centrales. Par exemple le « crypto-yuan » développé par la Chine. Plus d'infos

CFD

Contract For Difference, il s'agit d'un produit dérivé qui suit le cours d'un actif financier. Avec un CFD vous ne détenez pas l'actif en question, mais vous pariez sur sa hausse ou sa baisse et serez rémunérés sur l'écart de prix entre le moment de l'achat et celui de la vente. Un CFD vous autorise à utiliser des leviers ainsi que des shorts (ventes à découvert).

Chandelier japonais

Les chandeliers japonais, également appelés **« candlesticks** » en anglais, sont une méthode d'analyse technique populaire pour l'analyse des marchés financiers, tels que les marchés boursiers, les marchés des changes (Forex) et les marchés de la cryptomonnaie. Cette technique a été développée par les commerçants de riz japonais au XVIIe siècle, pour suivre

les fluctuations des prix de la céréale. Aujourd'hui, les chandeliers japonais sont largement utilisés pour l'analyse technique de tous les types de marchés financiers.

Chart

Il s'agit des graphiques des cours/prix des crypto-monnaies.

Clé privée

Une clé privée est une suite de lettres et de chiffres. Elle est stockée dans le portefeuille Bitcoin de l'utilisateur et à moins de faire l'effort d'aller la chercher et de l'exporter elle est généralement invisible pour l'utilisateur. Le portefeuille utilise cette clé privée pour signer les transactions envoyées afin de prouver que vous êtes bien le détenteur de celui-ci et des bitcoins qu'il contient, et que vous êtes autorisé à effectuer la transaction. On calcule la clé publique à partir de la clé privée. L'inverse est impossible.

Clé publique

Elle permet de recevoir des crypto-monnaies ou d'en envoyer. Cette clé peut prendre la forme d'une suite de lettres et de chiffres ou d'un QR code. On pourrait comparer la clé publique à un RIB/IBAN pour les monnaies classiques.

Coinbase

Coinbase est l'une des plus grandes plateformes d'échange de cryptomonnaies centralisées au monde. Créée en 2012 sous l'impulsion de Brian Armstrong (qui en est encore son PDG) et Fred Ehrsam, Coinbase est aussi l'une des premières à avoir vu le jou

Correction

Changement brutal du prix d'une crypto-monnaie qui se rapproche de son cours antérieur après une période de hausse ou de baisse relativement longue.

Cold storage

Technique pour conserver ses bitcoins en sécurité, hors ligne. Les clés privées sont créées et stockées dans un environnement sûr, hors ligne. En effet, les ordinateurs connectés (en ligne) sont vulnérables aux attaques informatiques. Plus d'infos

Colored coins

Protocole Bitcoin qui permet aux développeurs de créer des actifs numériques au-dessus de la blockchain Bitcoin pour des fonctions au-delà de la monnaie.

Confirmations

Quand une transaction est incluse dans un bloc, cela correspond à une confirmation. Quand un autre bloc est miné sur la même chaîne de blocs (blockchain) alors nous sommes à 2 confirmations et ainsi de suite.

Consensus

Quand la majorité des nœuds d'une blockchain ont les mêmes blocs dans leurs chaînes de blocs locales.

Coinbase & Coinbase Transaction

Coinbase : champ spécial utilisé comme unique entrée pour les *transactions coinbase*. Cela permet de récupérer la récompense de minage d'un bloc bitcoin et permet d'inclure jusqu'à 100 bytes de données.
Coinbase Transaction : la première transaction dans un bloc. Toujours créée par un mineur, elle inclut un seul coinbase.

CPU

Le Processeur (CPU en anglais) est le *cerveau* de l'ordinateur. La mémoire CPU était utilisée pour confirmer les transactions Bitcoin (minage). Aujourd'hui, ils ne sont plus assez performants pour cette tâche. Ils sont encore utilisés pour miner des altcoins.

Crypto-monnaie

Monnaie électronique pair à pair et décentralisée dont l'implémentation se base sur les principes de la cryptographie pour valider les transactions et la génération de la monnaie elle-même. À la différence des monnaies traditionnelles qui sont imprimées, les crypto-monnaies sont créées en résolvant des problèmes mathématiques basés sur la cryptographie.

Cryptographie

La cryptographie est une branche de mathématiques permettant de créer des codes et des chiffres qui peuvent être utilisés pour dissimuler l'information. La cryptographie sert de base dans les preuves mathématiques utilisées pour vérifier et sécuriser les transactions effectuées.

Curve War

Le terme Curve War, dans le contexte de la finance décentralisée (DeFi) et de Curve Finance, désigne une compétition entre différents protocoles DeFi construits en surcouche de Curve afin d'obtenir le plus de jetons CRV possible. Ces derniers peuvent être verrouillés dans le temps afin d'obtenir des veCRV, conférant ainsi un droit de vote au sein du protocole Curve. La détention de veCRV permet de :

- Voter pour la gouvernance de la DAO
- Voter pour l'allocation de l'émission monétaire du protocole au sein des différents pools

La Curve War consiste donc en une guerre d'influence parmi différents protocoles. Convex Finance est actuellement le premier détenteur de veCRV, ce qui lui confère un pouvoir de

vote important et la capacité d’orienter l’émission monétaire du protocole sur les pools de son choix.

Dapps (Application décentralisée) (

Une application décentralisée (Dapp) est une application qui s’exécute sur une blockchain (telle qu’Ethereum) de manière décentralisée, plutôt que sur des serveurs centralisés pour les applications traditionnelles. Pour cela, les Dapps utilisent des contrats intelligents (smart contract) pour interagir avec la blockchain et fournir des services à leurs utilisateurs. Les contrats intelligents sont des programmes informatiques autonomes et open-source qui sont exécutés automatiquement lorsqu’un ensemble de conditions prédéfinies est rempli (par
Les Dapps sont donc conçues pour être autonomes, sans avoir besoin de tiers pour stocker ou gérer les données qui y transitent. Elles sont ainsi résistantes à la censure et à la manipulation, car elles utilisent des protocoles de consensus décentralisés pour valider les transactions et garantir l’intégrité des données, sans qu’une autorité centrale ne puisse manipuler ses dernières (par exemple en refusant des paiements provenant d’une entité spécifique).
Ces applications sont accessibles via des portefeuilles de type « non custodial », tels que MetaMask, qui permettent aux utilisateurs d’interagir avec la blockchain.

DAO / Organisation décentralisée autonome

Une organisation décentralisée autonome (*Decentralized Autonomous Organization* – DAO) est un système de gouvernance qui repose sur la blockchain. Elle permet de démocratiser la prise de décision pour une communauté, en évitant de passer par un organisme centralisé.

Day Trading

Le fait d'acheter et de vendre sur des périodes allant de quelques heures à quelques jours pour profiter des baisses et montées des cours.

DEX

Acronyme de « Decentralized EXchange », les plateformes d'échange de cryptomonnaies décentralisées. Une telle plateforme est régie par des smart contracts et toutes les transactions sont consultables sur la blockchain. Les DEX ne vérifient pas l'identité de leurs utilisateurs, contrairement aux CEX. Les DEX les plus connus sont Uniswap, SushiSwap ou encore PancakeSwap.

DDoS / Attaque par Déni de Service

Une attaque DDoS est une attaque qui a pour but de rendre inaccessible ou inopérant un système informatique sur une durée de temps variable. Il est important que les exchanges soient résistants à ce type d'attaques.

Décentralisation

Dans le contexte du Bitcoin, la décentralisation est un enjeu permanent. Elle consiste à faire en sorte qu'aucune autorité centrale (entreprise, groupe d'individus, etc.) ne puisse avoir le contrôle du réseau. Plus il y a de nœuds appartenant à différentes entités sur le réseau, plus on considère que le réseau est décentralisé. Tout ceci est rendu possible grâce au fait que la Blockchain soit distribuée entre tous les nœuds du réseau. En apprendre davantage

DeFi / Finance Décentralisée

La finance décentralisée (DeFi) est un champ d'application des technologies blockchain. Elle rassemble des services de finance proposés sans organe de contrôle central, par exemple les prêts ou les oracles décentralisés.

Déflation

La déflation est la réduction des prix dans une économie au fur et à mesure que le temps s'écoule. Le Bitcoin avec son algorithme de création monétaire est déflationniste.

DevFee (Developer Fee)

Ce sont les frais avec lesquels les développeurs (propriétaires) d'un pool (groupement de mineurs) ou d'un programme de minage se rémunèrent. Les frais sont généralement compris entre 0 et 5%.

Difficulté

Dans le cas du Bitcoin, le réseau ajuste automatiquement la difficulté pour le minage via Proof-of-Work. Ainsi, plus la difficulté est élevée, plus il faudra de puissance pour résoudre la preuve de travail. Cette difficulté est recalculée tous les 2016 blocs soit toutes les 2 semaines (pour rappel un bloc est créé toutes les 10 minutes).

Dip

Il s'agit d'une chute brutale et éphémère du cours qui retrouve très rapidement sa valeur. Cela peut correspondre à une vente importante par une baleine. Les dips peuvent constituer de bonnes opportunités pour ceux qui ont placé des ordres d'achat. L'expression ***Buy The Fucking Dip*** consiste à acheter les points les plus bas dans un marché haussier.

Double dépense

Lorsqu'une personne essaye d'envoyer une transaction à deux destinataires en même temps. L'objectif étant de dépenser des bitcoins qu'on ne possède pas. Pour cela il est nécessaire d'obtenir une puissance de calcul élevée afin que les blocs contenant les transactions soient validés alors qu'ils ne le devraient pas. En savoir plus

Dump

Baisse du prix d'une crypto-monnaie

DYOR
DYOR est un acronyme anglais signifiant « Do Your Own Research », qui se traduit en français par « Faites Votre Propre Recherche ». Cette expression est souvent utilisée dans les communautés liées aux cryptomonnaies et aux investissements de manière générale, pour rappeler aux investisseurs l'importance de faire leur propre analyse avant de prendre une décision d'investissement

Ethereum

Ethereum est une plateforme, semblable à un « ordinateur mondial », sur laquelle on peut exécuter des applications sans avoir recours à un serveur centralisé. Chaque nœud de la blockchain est chargé d'une partie de l'exécution des applications présentes sur celle-ci. À l'instar de Bitcoin qui n'a pas besoin d'intermédiaire (banque) pour échanger des unités monétaires, Ethereum offre des services qui n'ont plus besoin d'intermédiaires pour être exécutés. Ethereum vise à bâtir un Web où les intermédiaires entre les clients et les services qu'ils recherchent n'existent plus. Il serait par exemple possible de commander un chauffeur sans passer par un service comme Uber qui prend une commission à chaque trajet/transaction pour la mise en relation du client et du chauffeur. La blockchain Ethereum fonctionne avec la crypto-monnaie Ether dont le sigle est l'ETH.

ECDSA

Elliptic Curve Digital Signature Algorithm est un algorithme cryptographique utilisé par Bitcoin pour s'assurer que les fonds peuvent uniquement être dépensés par leurs propriétaires.

Equity token
Un equity token est un type de jeton qui représente une participation en capital dans une entreprise ou une organisation. Contrairement aux autres types de jetons, tels que les jetons utilitaires ou les jetons de sécurité, les equity tokens donnent à leurs détenteurs une part de propriété dans l'entreprise qui les a émis.

ERC-20 (Token)

ERC signifie Ethereum Request for Comments. Il s'agit d'un protocole officiel pour proposer des améliorations au réseau Ethereum. Les tokens issus de ce protocole ont
pour *objectif* d'améliorer Ethereum. Pourquoi le chiffre 20 ? Car c'est la proposition portant ce numéro qui fut postée sur le Github et retenue par la communauté. ERC20 définit un ensemble de règles qui doivent être respectées pour qu'un token soit accepté et appelé token ERC20.

ERC-721 (Token)

Les tokens ERC-721 sont une catégorie de tokens Ethereum. Il s'agit de tokens non fongibles (NFT), qui sont particulièrement utilisés dans les jeux vidéo blockchain.
C'est une place de marché où l'on échange des cryptos-monnaies entre elles ou contre des monnaies fiduciaires. Cela permet d'investir ou de spéculer sur le cours des crypto-monnaies.

Exit scam

L’exit scam, qu’on traduit par « escroquerie de sortie » en français, est un type d’arnaques aux cryptomonnaies. Les arnaqueurs récoltent les fonds des investisseurs contre la promesse d’un produit fini, puis ils s’éclipsent en gardant l’argent, sans délivrer de produit. Les exit scams ont été particulièrement nombreux lors de l’essor des ICO en 2017 et 2018.

Faucet / Robinet

Les Faucets sont des sites qui distribuent gratuitement des tokens dans le but de démocratiser l'utilisation d'une monnaie et d'attirer le chaland.

Fees / Frais

Il s'agit des frais de transactions appliqués par les Exchanges lors de l'achat/vente de crypto-monnaies. Le Bitcoin contient également des frais de transaction minimes qui sont redistribués aux mineurs.

Ferme de Minage

Les fermes de minages sont des entrepôts regroupant des centaines de mineurs (ASIC en général). Leur hashrate est tellement important qu'il est parfois équivalent à quelques pourcents du hashrate total de la Blockchain sur laquelle elles minent.

Fiat / Monnaie Fiduciaire

La monnaie fiduciaire est la monnaie classique comprenant les pièces et les billets de banque : euros, dollars, etc.

Flippening

Le « flippening » est un terme qui désigne un scénario hypothétique dans lequel la capitalisation boursière de l’Ethereum (ETH) dépasse celle du Bitcoin (BTC), faisant de l’ETH la cryptomonnaie la plus valorisée du marché. Le flippening est un sujet de discussion populaire dans la communauté des cryptomonnaies depuis plusieurs années, et bien que la capitalisation boursière de l’Ethereum ait atteint un niveau record par rapport au Bitcoin en 2017 et en 2018, le bitcoin reste actuellement la cryptomonnaie la plus valorisée en termes de capitalisation boursière.

FOMO (Fear Of Missing Out)

FOMO est l'acronyme anglais qui représente la peur de manquer quelque chose. Cela se produit lorsqu'une décision est prise de façon impulsive par peur de rater une bonne affaire.

Fongibilité

Capacité d'un bien ou d'un actif à être échangé avec d'autres biens ou actifs individuels de même type. Par exemple, les jetons bitcoin sont fongibles.

Forgeur

Personne ou groupe de personnes qui connectent sur le réseau une ou plusieurs machines pour effectuer du minting (forgeage).

Fork

La création d'une version alternative de la blockchain. La cause de cette bifurcation peut être soit malveillante, soit accidentelle, suite a un bug ou bien encore intentionnelle quand les développeurs décident d'introduire de nouvelles fonctionnalités. La version la plus longue de la blockchain devient la version principale.
Hard Fork : Séparation de la chaîne de blocs (split) en deux parties pouvant aboutir à la création de deux monnaies distinctes, mais avec un historique commun. Un hard fork très connu est celui de l'ETC pour créer l'ETH, suite à un désaccord de vision sur l'immutabilité de la blockchain.
Soft Fork : Modification mineure de la chaîne de blocs sans séparation en deux parties (split). Par exemple, le segwit est implémenté via un soft fork.

FUD (Fear, Uncertainty and Doubt)

Le FUD (littéralement « peur, incertitude et doute ») est une technique rhétorique utilisée notamment dans la vente, le marketing, les relations publiques et le discours politique. Elle consiste à tenter d'influencer autrui en diffusant des informations négatives, souvent vagues et inspirant la peur. Le FUD peut être utilisé comme une stratégie pour dénigrer une crypto-monnaie ou un projet.

Gas

Lorsqu'on veut utiliser un smart contract sur le réseau Ethereum, il faut utiliser de la puissance de calcul. Le gas représente le temps de travail informatique nécessaire pour mener à bien une telle opération. C'est le prix qu'on va payer pour utiliser le smart-contract, il varie en fonction du type de contrat intelligent.

GMX

GMX est un protocole décentralisé d’échange de cryptomonnaies, également appelé DEX (Decentralized Exchange). Il s’agit d’une plateforme utilisant la blockchain qui permet aux utilisateurs d’échanger des actifs numériques directement entre eux sans passer par un intermédiaire centralisé comme une plateforme d’échange traditionnelle.

(Problème des) Généraux Byzantins

Un réseau continue de fonctionner correctement même si un des « piliers » (dans le cas du Bitcoin un noeud) est corrompu, fonctionne mal ou n'existe plus.

Gossip Protocol

Algorithme P2P (pair à pair) pour distribuer une information à tous les participants du réseau.

GPU (Graphical Processing Unit)

Le processeur graphique ou GPU (Graphical Processing Unit en anglais) est un circuit intégré conçu pour assurer les fonctions de calculs complexes nécessaires à l'affichage des millions de polygones dans les graphiques des jeux vidéo modernes. Le GPU est également adapté aux calculs cryptographiques nécessaires au minage des crypto-monnaies.

Halving

On parle de halving lorsque la récompense de minage d'une crypto-monnaie est divisée par deux. Cet évènement est programmé à l'avance dans le code de la monnaie et se déclenche automatiquement lorsqu'un certain nombre de blocs ont été minés.
Par exemple pour le Bitcoin : La prime de minage est divisée par deux tous les 210 000 blocs de transactions minés. Les premiers mineurs gagnaient 50 BTC par bloc généré, puis cette valeur est passée à 25 BTC en 2012 et à 12,5 BTC en 2016. Le prochain halving du Bitcoin est prévu en juillet 2020 (il s'agit d'une date prévisionnelle).

Hardware wallet

Portefeuille physique qui permet de conserver ses clés privées dans un équipement informatique.

Hachage

Un procédé mathématique qui, à partir d'une quantité de données en entrée, produit une sortie de taille fixe. La fonction de hachage a deux caractéristiques importantes : premièrement, il est mathématiquement difficile d'identifier la donnée initiale en regardant la donnée de sortie ; deuxièmement, en changeant une infime partie de l'entrée initiale, la donnée de sortie est alors complètement changée. Le *hash* est le résultat d'une fonction de hashage.

Hashrate

Cela détermine la puissance d'un mineur ou bien d'un réseau. C'est grâce à ce taux que la difficulté s'ajuste.

Hodl

Il y a plusieurs années, un individu ivre a posté un message sur BitcoinTalk (un forum spécialisé dans le Bitcoin) et a écrit plusieurs fois **hodl** à la place de **hold**. Un mème était né.

Hold

Le fait de garder une crypto-monnaie et de ne pas la vendre, quelles que soient les variations du cours (hausse/baisse). Les individus qui ont acheté des bitcoins en 2010 et qui hold toujours ont fait une importante plus-value.

ICO (Initial Coin Offering)

Une ICO (Initial Coin Offering) est une méthode de distribution de tokens via une levée de fonds. Elle est utilisée pour le lancement de projets liés aux crypto-monnaies et à la

blockchain. Lors d'une ICO, les investisseurs peuvent acheter des tokens, ce qui est similaire au fait d'acheter des parts dans une société classique. Cela permet au projet de lever des fonds, et cela permet aux investisseurs de prendre part au projet et de spéculer sur sa future valeur.

IDO (Initial DEX Offering)

Une IDO (Initial Dex Offering) fonctionne presque de la même manière qu'une ICO, sauf que la levée de fonds se déroule sur une plateforme décentralisée et ne nécessite pas, du moins le plus souvent, de faire vérifier son identité.

IEO (Initial Exchange Offering)

Une IEO (Initial Exchange Offering) est une autre variante de l'ICO. Un IEO se déroule sur une plateforme d'échange centralisée, comme son nom l'indique. Pour y participer, il faudra nécessairement disposer dans son portefeuille de tokens liés à la plateforme. Par exemple, dans le cas des IEO de Binance, seuls les utilisateurs qui disposent de BNB dans leurs portefeuilles peuvent y participer.

Justin Sun

Justin Sun est un entrepreneur chinois, très influent dans le monde de la blockchain. Il est surtout connu pour être le fondateur et le PDG de TRON, une blockchain qui vise à créer un écosystème décentralisé de contenu en ligne.

KYC

KYC (**Know Your Customer en anglais** = « Connaissez votre client » en français) est un processus qui consiste à vérifier l'identité des clients d'une entreprise. Cette pratique permet à une entreprise de s'assurer que ses clients sont réels et légitimes, et qu'ils ne sont pas impliqués dans des activités criminelles telles que le blanchiment d'argent, le financement du terrorisme ou la fraude.

Lambo

Il s'agit d'un mème. Tous les **traders en crypto-monnaies** s'achèteront une Lamborghini lorsqu'ils seront riches.

Last

Sur un exchange, cela désigne généralement le dernier prix auquel a été échangée une crypto-monnaie donnée.

Laszlo Hanyecz

Laszlo est un développeur connu pour avoir réalisé le premier achat en bitcoins dans le monde réel. Il a acheté 2 pizzas pour 10.000 BTC le 22 mai 2010, ce jour est alors célébré dans la sphère crypto comme étant le **Bitcoin Pizza Day**. Fait moins connu, Laszlo est également le premier mineur GPU de l'histoire.

Layer 1

La couche 1, ou layer 1, décrit l'architecture principale sous-jacente d'une blockchain. Par exemple, Bitcoin et Ethereum sont des layers 1.

Layer 2

La couche 2, ou layer 2, décrit un réseau superposé qui se branche au-dessus d'une blockchain en layer 1. Par exemple, le Lightning Network est un layer 2 de Bitcoin, de même avec Arbitrum qui se branche au-dessus de la blockchain Ethereum.

Lending

Le lending correspond à l'action de faire des prêts qui utilisent des cryptomonnaies comme le Bitcoin ou des stablecoins en tant que garantie, plus communément appelé « collatéral ». Les utilisateurs qui emprunte des fonds avec ce mécanisme.

Levier

En finance, un levier est synonyme de multiplicateur, la plateforme va vous prêter des liquidités pour augmenter la taille de vos positions. Ainsi si vous avez mis 100$ en levier x5 cela équivaut à avoir une position de 500$. Un levier est dangereux, bien que vos gains peuvent être multipliés il en est de même pour vos pertes. Soyez très vigilants avec les effets de levier.

Limit Buy / Limit Sell

Ordre d'achat placé par un investisseur qui souhaite acheter/vendre des crypto-monnaies à un prix fixé à l'avance.

Long

Faire un long consiste à miser à la hausse du cours en utilisant le margin trading. C'est-à-dire emprunter de l'argent à un instant t, en espérant que le prix augmente afin de rembourser les montants empruntés tout en dégageant un profit.

LTF

LFT qui est l’acronyme de « Low time frame » en anglais et signifie « petite échelle de temps » en français. Dans le domaine du trading, et notamment de la cryptomonnaie, LTF est utilisé pour décrire une approche d’analyse de marché basée sur une période de temps courte.

Un « Low Time Frame » s’oppose à un « High Time Frame », qui est une période de temps plus longue et plus globale.

Luck (Mining)

Pourcentage de chance (sur une durée définie) selon lequel un mineur ou un pool trouve un bloc. Le pourcentage peut varier entre 0% et +∞%. Dans un monde *parfait*, la Luck serait systématiquement de 100%.

Mainnet

Dans le domaine des technologies de registre distribué, le terme « mainnet » est utilisé pour désigner le réseau principal d'une blockchain. Le mainnet est le réseau sur lequel les transactions sont effectuées, les blocs sont validés et les jetons sont échangés par l'ensemble des utilisateurs.
Lorsqu'une nouvelle blockchain est créée, elle commence généralement par un « testnet », qui est un environnement de test pour les développeurs et les utilisateurs, dont l'objectif est de s'assurer que le réseau fonctionne comme il se doit avant son lancement officiel. Pour certaines blockchains, notamment Ethereum, il existe une multitude de testnets permettant de renforcer la phase de test avant toute mise à jour d'envergure. Une fois que la blockchain est prête pour une utilisation en production, le mainnet est lancé et les utilisateurs peuvent commencer à effectuer des transactions réelles sur le réseau.

Margin Trading

Méthode risquée qui consiste à emprunter de l'argent pour faire du trading. A pour effet d'amplifier les gains et les pertes.

Market Buy

Il s'agit de l'ordre d'achat au meilleur prix de marché à l'instant de l'achat. À opposer au *market sell*

Market Cap

Représente la capitalisation d'une crypto-monnaie ou d'un ensemble de crypto-monnaies (le montant total en circulation). Pour obtenir le market cap d'une crypto-monnaie il faut multiplier le nombre d'unités en circulation par le prix à l'unité.

Market Sell

Il s'agit de l'ordre de vente au meilleur prix de marché à l'instant de la vente. À opposer au *market buy*.

Maximalist Bitcoin

Un « maximalist », ou « Bitcoin maximalist » est un amateur de Bitcoin (BTC) qui considère qu'il s'agit de la seule crypto-monnaie viable, et que toutes les autres sont vouées à disparaître. Le mot peut également désigner un investisseur qui mise tout sur le BTC, sans diversifier son portfolio.

Métavers / Metaverse

Le métavers (ou metaverse en anglais) est un concept d'univers virtuel en ligne et en 3D, qui, le plus souvent, combine ses éléments avec la technologie des tokens non fongibles (NFTs). Au sein d'un métavers, les utilisateurs peuvent se rencontrer à travers d'avatars virtuels, pour des activités diverses : travaille, jouer, assister à un concert, etc.

Mineur

Personne ou groupe de personnes qui connectent sur le réseau une ou plusieurs machines pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau.

Mining / Minage

Processus permettant de résoudre un défi informatique imposé par une Proof of Work (PoW). L'utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés. Le minage est récompensé par la génération/distribution de nouveaux bitcoins/altcoins.

Minting / Forgeage

Processus permettant de résoudre un défi informatique imposé par une Proof of Stake (PoS). L'utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés. Le minage est récompensé par la génération/distribution de nouveaux bitcoins/altcoins.

Minage en Pool

Processus de minage où des mineurs se regroupent pour miner ensemble et soumettre leurs hashs au réseau de façon collective. La rémunération est alors partagée équitablement entre les mineurs selon la contribution de chacun. Ce processus est connu pour avoir un caractère aléatoire presque nul et une rémunération beaucoup plus fréquente et régulière, mais aussi moins importante.

Minage en Solo

Processus de minage où un mineur soumet ses hashs directement au réseau et est rémunéré seul. Ce processus est connu pour avoir un caractère aléatoire plus important, mais aussi une rémunération beaucoup plus importante.

Mt. Gox

À l'origine il s'agissait d'une plateforme d'échange de cartes *Magic the Gathering*, qui après son rachat par le français Mark Karpeles est devenue l'exchange de bitcoins le plus connu au monde. La plateforme a été victime d'une attaque informatique causant la perte d'une grande partie des bitcoins stockés en ligne. Mt. Gox a été placé en liquidation judiciaire.

Move to earn

Le move to earn (qui signifie « bouger pour gagner » en français) est un concept qui associe des éléments issus des jeux vidéo et des applications de fitness pour récompenser les utilisateurs ayant une activité physique. Il s'inspire du play to earn, qui consiste à gagner des cryptomonnaies en jouant à des jeux basés sur la blockchain.
Le move to earn utilise généralement un appareil mobile connecté qui enregistre les données de déplacement des utilisateurs, comme la distance parcourue, le nombre de pas, les calories brûlées, etc. Ces données sont ensuite converties en tokens ou en points qui peuvent être échangés contre des récompenses, comme des NFT, des objets virtuels, des services ou d'autres cryptomonnaies.

NGMI

Acronyme « Not Gonna Make It ». Ce terme est utilisé lorsqu'une personne veut montrer son désaccord avec une certaine action ou en témoignage de sa déception à l'égard d'une mauvaise décision. NGMI est souvent utilisé par la communauté des tokens non fongibles.

Node / Noeud

Dans un réseau informatique, cela représente une machine qui fait partie du réseau.

Nonce

Dans le domaine de la cryptographie, le terme « nonce » est utilisé pour désigner un nombre aléatoire qui est utilisé une seule fois dans un contexte spécifique, comme par exemple lors de la création d'un nouveau bloc sur un réseau blockchain

NFT (Non Fungible Token)

C'est un token qui a des propriétés spécifiques et qui ne peut pas être échangé contre un autre jeton aux mêmes caractéristiques.

Oracle (blockchain)

Dans l'écosystème des cryptomonnaies et de la blockchain, un oracle est un agent ou un service tiers qui achemine des données externes vers une blockchain ou des contrats intelligents (smart contract). Ces entités intermédiaires sont nécessaires car les blockchains ne peuvent pas accéder aux données extérieures de manière native en raison de leur conception sécurisée et décentralisée.

OTC (Over The Counter)

Il s'agit d'un échange ad hoc entre deux personnes, c'est-à-dire sans intermédiaire.

P2P (Peer-to-Peer) / Pair-à-pair

Les systèmes peer-to-peer permettent à plusieurs ordinateurs de communiquer entre eux via un réseau en y partageant des informations. La particularité des architectures peer-to-peer réside dans le fait que les données sont transférées directement entre deux postes connectés au réseau, sans transiter par un serveur central. Il permet ainsi à tous les ordinateurs de jouer directement le rôle de client et de serveur. On appelle souvent *nœud* les postes connectés par

un réseau peer-to-peer. Le protocole BitTorrent utilise le système peer-to-peer tout comme le Bitcoin.

Panic Buy

Se dépêcher d'acheter une crypto-monnaie sans prendre le temps de la réflexion par peur de louper une bonne affaire. Par exemple, lorsqu'une news vient de paraître ou lorsqu'il y a un pump.

Panic Sell

Se dépêcher de vendre une crypto-monnaie sans prendre le temps de la réflexion par peur que le cours baisse. Par exemple, pour essayer de limiter la perte lorsqu'une mauvaise news vient de paraître ou lorsqu'il y a un dump.

Pool

Il s'agit d'un regroupement de mineurs qui mettent en commun leur puissance de calcul afin d'augmenter leur capacité de résolution des blocs d'unn blockchain. Les gains générés sont partagés entre les mineurs du pool.

Pool de liquidité

Un pool de liquidité est l'un des éléments clés de la finance décentralisé et plus particulièrement des DEX. C'est à l'intérieur de ces pools que sont déposés des tokens afin de faciliter leur trading. Les utilisateurs que l'on nomme fournisseurs de liquidités (LP) ajoutent une valeur égale de deux tokens (50% USDC / 50% ETH par exemple) dans un pool pour créer une paire sur un DEX. En échange, ils reçoivent une partie des frais payés par les utilisateurs de la pool de liquidité, en fonction de leur contribution.

PoS (Proof of Stake) / Preuve d'Enjeu

La preuve d'enjeu est une alternative au mécanisme de preuve de travail (Proof of Work), qui est souvent critiqué pour son coût en électricité et son impact environnemental. L'algorithme de la preuve d'enjeu tente de résoudre ces problèmes en supprimant entièrement le concept de minage et en le remplaçant par un mécanisme de *minage virtuel*. La preuve d'enjeu demande à l'utilisateur de prouver qu'il possède une certaine quantité d'une crypto-monnaie donnée afin d'obtenir le droit de valider des blocs supplémentaires. L'algorithme va sélectionner aléatoirement un validateur parmi les personnes éligibles (plus une personne possède une grande quantité de la crypto-monnaie plus elle a de chances d'être sélectionnée) et va lui attribuer le droit de créer le prochain bloc. Tout comme dans le mécanisme de preuve de travail, la chaîne la plus longue est par défaut considérée comme la chaîne valide.

PoW (Proof of Work) / Preuve de Travail

Système permettant de dissuader le spam et les attaques DDoS en requérant de la puissance de calcul par ordinateur au demandeur de service. Ce système est caractérisé par l'asymétrie du coût de calcul : le travail doit être difficilement réalisable pour le demandeur, mais facilement

vérifiable par un tiers. Dans le domaine des crypto-monnaies, cette méthode de validation par preuve de travail est utilisée pour ajouter un bloc supplémentaire à la chaîne de blocs, chaque mineur du réseau doit réaliser des calculs coûteux en temps et en énergie afin de chiffrer l'ensemble des transactions d'un bloc ainsi que les transactions chiffrées de la chaîne de bloc précédente. Lorsque la solution est validée, elle est diffusée à l'ensemble du réseau. Le mineur ayant trouvé la solution est récompensé en monnaie nouvelle selon les modalités définies par le protocole de la crypto-monnaie. La falsification d'une preuve de travail est difficile, voire impossible.

Pré-minage

Les crypto-monnaies sont parfois pré-minées, c'est-à-dire que les développeurs minent des blocs avant de sortir publiquement la crypto-monnaie.

Proof Of History

Le Proof of History (Preuve d'Historique) est un mécanisme de consensus utilisé dans les blockchains pour garantir que les données historiques sont exactes et n'ont pas été falsifiées. Ce mécanisme est utilisé par la blockchain Solana, en combinaison avec le Proof of Stake. Horodater le registre de façon infaillible est l'une des préoccupations majeures de toutes les blockchains.

Pump

Hausse du prix d'une monnaie

Refill

Racheter une certaine quantité d'une crypto-monnaie que l'on possède déjà à un prix que l'on juge intéressant.

Rig de Minage

Ce sont des mineurs composés de plusieurs GPU, la configuration la plus répandue est celle qui contient 6 GPU. Les rigs de minage dégagent généralement un hashrate équivalent a 0.000X% du hashrate total de la Blockchain sur laquelle elles minent.

Ripple (XRP)

Système de paiement construit sur un protocole Internet distribué et open source et basé sur une cryptomonnaie appelée XRP. Lancé en 2012, le réseau Ripple vise à permettre des transactions financières mondiales sécurisées, instantanées et presque gratuites.

ROI (Return on Investment)

Il est calculé en faisant le rapport du profit réalisé sur le montant investi. Un ROI de 100% signifie que l'on a doublé sa mise de départ.

Root

Dans le domaine de la cryptographie, le terme « root » est souvent utilisé pour désigner la « racine » d'un arbre de hachage, également appelé arbre de Merkle (ou « Merkle tree » en anglais). Un arbre de Merkle est une structure de données utilisée pour vérifier l'‘intégrité des données stockées dans un système informatique, comme une blockchain. Cette dernière est construite grâce à l'addition successive de blocs les uns après les autres. Au sein de chaque bloc, un arbre de Merkle est construit à partir des hashes de chaque transaction, ajoutés 2 à 2 puis hashés de nouveau jusqu'à obtenir le dernier hash. Ce tout dernier hash correspond à la racine de l'arbre, et est toujours ajouté dans l'entête du bloc.

Rug Pull

Le terme *rug pull*, littéralement « tirer le tapis » en français, désigne une arnaque courante dans l'espace des cryptomonnaies où les développeurs d'un projet de cryptomonnaie ou d'une application décentralisée (dApp) drainent soudainement les fonds d'un pool de liquidité ou d'un portefeuille d'investissement, laissant les investisseurs avec des actifs sans valeur et sans moyen de récupérer leur investissement initial.

Satoshi

Un satoshi représente la plus petite unité du Bitcoin (1 satoshi = 0,00000001 BTC). C'est une unité souvent utilisée dans le milieu du trading. Elle fait référence au créateur de Bitcoin : Satoshi Nakamoto.

Satoshi Nakamoto

Satoshi Nakamoto est le pseudonyme de la personne qui a créé Bitcoin. C'est aussi le fondateur du site Web *Bitcoin.org* et du forum *BitcoinTalk*. À ce jour, on ne sait toujours pas qui se cache sous ce pseudonyme. Est-ce une seule et même personne ? Un groupe de cryptographes ? Une entité gouvernementale ? Nul ne le sait.

Scalabilité

La scalabilité, ou mise à l'échelle, est la capacité d'une blockchain à s'adapter à un nombre croissant d'utilisateurs et de transactions. Il s'agit d'une problématique à laquelle se heurtent beaucoup de blockchains, dont Bitcoin et Ethereum. En savoir plus

Scalping

Le fait d'acheter et de vendre sur de courtes périodes pour profiter des fluctuations du cours pour faire des profits.

Scam / Arnaque

Un *scam* est une escroquerie sur Internet. Les exemples les plus courants dans le monde des crypto-monnaies sont les levées de fonds pour un projet (ICO) où les fondateurs du projet disparaissent avec l'argent récolté.

Segwit (Segregated Witness)

Un *Segwit* est un soft-fork d'une crypto-monnaie, qui permet de changer le format des transactions dans la blockchain, afin d'augmenter la capacité d'un block, ainsi que la sécurité des transactions

SHA-256

SHA-256 est une fonction cryptographique utilisée comme la base du système de preuve de travail du Bitcoin.

Sharding

Le sharding (partitionnement en français) est une solution de scalabilité développée pour le réseau Ethereum. Elle permet de fragmenter les données utilisées sur le réseau, afin d'améliorer sa capacité de travail.

Share

Morceau, part, qu'un mineur aura méritée selon la contribution qu'il aura fournie à son pool de minage.

Shitcoin

Désigne une crypto-monnaie qui n'a aucune base technique sérieuse, qui ne repose sur rien de concret et qui ne sert qu'à spéculer ou arnaquer les débutants.

Short

Parier sur la baisse du cours. L'investisseur anticipe la baisse du cours et vend des crypto-monnaies afin de les racheter à un prix plus bas.

Sidechain

Il s'agit d'une blockchain secondaire qui se développe parallèlement à une blockchain principale, mais qui y est rattachée afin de pouvoir en connaitre toutes les informations. Les *sidechains* permettent d'accroître le volume d'informations pouvant être traitées au sein d'une blockchain (volume normalement limité), tout en restant sur une même blockchain principale.

Silk Road

Silk Road était un marché noir en ligne, généralement utilisé pour effectuer des achats illicites, souvent avec des crypto-monnaies comme le Bitcoin. *Silk Road* a été saisi et fermé en octobre 2013 par le FBI et son propriétaire Ross Ulbricht a été arrêté et condamné à la prison à perpétuité.

Slippage

Dérapage, lorsque le volume d'échange est trop important ou que des positions entrent en phase de liquidation il est possible de voir le prix exploser dans un sens. Cela peut être tellement rapide et puissant que la plateforme peut être surchargée et votre ordre peut s'exécuter en retard. Un stop-loss ou toute forme d'ordre peut s'activer bien trop tard et vous faire perdre plus que prévu. On appelle ceci l'effet de glissement ou slippage en anglais.

Smart Contract / Contrat Intelligent

Les *smart contrats* sont des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable. Ils fonctionnent comme toute instruction conditionnelle de type « if – then » (si telle condition est vérifiée, alors telle conséquence s'exécute). On dit souvent que, si la blockchain est un tableau Excel, alors les *smart contracts* sont des macros. Ces contrats intelligents s'appuient sur la technologie blockchain du réseau Ethereum pour rendre infalsifiables les termes et les conditions de leur exécution.
Un exemple pratique : imaginons que vous souhaitez réaliser un site permettant à chacun d'effectuer un pari. Vous réalisez un contrat qui contient les instructions suivantes :
- Si quelqu'un envoie de l'ether et parie sur « PSG », enregistrer son pari et calculer une nouvelle cote ;
- Si quelqu'un envoie de l'ether et parie sur « OM », enregistrer son pari et calculer une nouvelle cote ;
- À l'issue du match, consulter une base de données fiable contenant le résultat du match et distribuer les gains mathématiquement en fonction des cotes et des paris de chacun.
Une fois le programme créé, il peut s'exécuter de façon entièrement automatique et vérifiable par chacun. C'est un système de pari totalement transparent et décentralisé. Comment les contrats sont-ils exécutés ? Pour exécuter les instructions sur la blockchain Ethereum, il faut de la puissance de calcul. Cette puissance de calcul est fournie par les participants au réseau. Ce sont des particuliers ou des entreprises qui décident de mettre à la disposition du réseau leur ordinateur pour faire fonctionner la blockchain. Ils sont rémunérés pour cela, par l'octroi d'ethers.

Solidity

C'est le langage de programmation orienté objet utilisé pour écrire des smart-contracts ou contrats intelligents ainsi que des DApps (applications décentralisées). Il est utilisé dans de nombreuses blockchains, mais à l'origine pour celle d'Ethereum. Découvrir Solidity

Spread

Le *spread* représente la différence de prix entre l'offre d'achat (bid) et l'offre de vente (ask) les plus proches. Il est exprimé en pourcentage.

Stack

Désigne l'ensemble du capital en crypto-monnaies possédé par un investisseur.

Staking

Le staking est un procédé rendu possible par le consensus Proof-of-Stake (PoS). Pour faire du staking, un utilisateur verrouille une partie de ses crypto-monnaies. Celles-ci ne peuvent plus être utilisées, mais elles contribuent à soutenir les opérations du réseau. En échange de ce travail, l'utilisateur reçoit des récompenses de « staking », qui sont proportionnelles au nombre de tokens qu'il a verrouillés.

Stop Loss

Il définit la perte maximale acceptable par l'investisseur. Généralement, un investisseur placera un stop loss à 5% en dessous de son prix d'achat afin de solder **automatiquement** sa position en cas de perte. Le stop loss est très utilisé par les investisseurs qui font du scalping/day trading, mais beaucoup moins par les holders qui visent le long terme. Le stop loss est à opposer au take profit.

Support

Zone à partir de laquelle le marché estime que le prix d'achat est correct et où de nombreux ordres sont placés faisant office de supports.

Swap

Les swap de tokens, se refaire à un échange direct d'une certaine quantité d'un token contre un autre. Cette action se fait de manière décentralisée, via un protocole comme Uniswap ou SushiSwap, dont la liquidité des paires supportées de tokens est alimentée par les utilisateurs.

Take Profit

Il définit le gain minimum souhaité par l'investisseur. Généralement, un investisseur placera un take profit à 5% au-dessus de son prix d'achat afin de solder **automatiquement** sa position en cas de hausse du cours. Le take profit est très utilisé par les investisseurs qui font du scalping/day trading, mais beaucoup moins par les holders qui visent le long terme. Le take profit est à opposer au stop loss.

Testnet

Testnet est une alternative à la Blockchain du réseau Bitcoin, utilisée uniquement pour effectuer des tests sur le protocole et le réseau sans que cela n'ait d'influences concrètes pour les utilisateurs.

To theMoon

Il s'agit d'un mème. Lorsqu'on croit à une crypto-monnaie ou lorsqu'un pump a lieu, on dit de celle-ci qu'elle atteindra la Lune : **to the Moon**.

Tokens / Jetons

Les tokens sont propres à chaque crypto-monnaies ou projets. Par exemple, les bitcoins sont les tokens du réseau Bitcoin et les ethers sont les tokens du réseau Ethereum.

Top / Sommet

Le top (sommet en français) est le prix le plus élevé qu'un actif pourra atteindre avant de repartir à la baisse. Il s'oppose au bottom (creux).

TOR (The Onion Router) / Le Routage en Oignon

TOR est un réseau informatique mondial et décentralisé qui permet de naviguer de façon anonyme sur Internet grâce à des relais.

Trading Bot

Programme informatique configuré pour passer des ordres d'achats et de ventes automatiques (sans intervention humaine) en fonction de paramétrages définis à l'avance par son programmeur.

Uptrend

Uptrend est un terme utilisé dans l'analyse technique des marchés financiers pour décrire une tendance haussière des prix d'un actif financier, tel que les cryptomonnaies. Les prix montent de manière constante sur une période prolongée, caractérisée par une série de sommets et de creux qui se situent à des niveaux de prix de plus en plus élevés. Cette tendance est souvent considérée comme un signal d'achat, car elle indique que les prix ont une forte probabilité de continuer à augmenter.

UTXO

UTXO, ou **Unspent Transaction Output**, est un terme utilisé dans le domaine de la blockchain et des cryptomonnaies pour décrire une sortie de transaction non dépensée. Toutes les blockchains n'utilisent pas le système UTXO mais c'est le cas de Bitcoin notamment. Sur ce dernier, chaque transaction est composée d'une ou plusieurs entrées et sorties, chaque entrée étant la sortie d'une autre transaction, hormis pour le cas très spécifique de la création des nouveaux bitcoins à chaque bloc. La monnaie bitcoin est donc constituée de l'ensemble des UTXO, et la somme de tous les UTXO disponibles à une adresse publique correspond à son solde disponibl

Vanity Address

Correspond à une adresse bitcoin personnalisée, à opposer aux adresses classiques qui sont générées de façon aléatoire

Vitalik Buterin

Vitalik Buterin, né le 31 janvier 1994, est un programmeur russo-canadien. Il est connu en tant que co-fondateur d'Ethereum et de Bitcoin Magazine. Il a reçu en 2014 le prix *Pether Thiel Fellowship* pour son travail et figure dans la liste du magazine *Fortune de moins de 40 ans*.

Volatilité

Lorsque le cours d'une crypto-monnaie varie beaucoup, on dit de lui qu'il est volatile.

WAGMI

Acronyme de « We All Gonna Make It », une phrase très utilisée au sein de la communauté des tokens non fongibles. Dire « WAGMI traduit un état optimiste concernant l'avenir d'un investissement. »

Wall / Mur

Un *wall* est représenté par un important ordre d'achat/vente. On utilise ce terme, car un mur se dessine lorsqu'on regarde l'order book.

Wallet / Portefeuille

Un *wallet* est un portefeuille dans lequel il est possible de stocker des crypto-monnaies. Il existe des portefeuilles en ligne sur des exchanges tels que Coinbase et Kraken. Mais il existe également des portefeuilles privés qui permettent de stocker des crypto-monnaies par ses propres moyens sans faire appel à un intermédiaire.

Weak Hands

Représente les personnes qui paniquent facilement et vendent à la moindre rumeur ou dès que le cours d'une crypto-monnaie baisse (quitte à perdre de l'argent).

Web 1.0

Le terme « Web 1.0 » désigne la première étape de l'évolution d'Internet.

Web 2.0

Le « Web 2.0 » apporte les notions d'intéropérabilité entre les utilisateurs avec l'arrivée des réseaux sociaux et des plateformes comme YouTube. Il fait référence au Web d'aujourd'hui, majoritairement contrôlé par des grandes entreprises comme Google, Amazon ou encore Facebook. Il est particulièrement centralisé et la censure y est présente.

Web 3.0

Le « Web 3.0 » apporte la décentralisation à l'écosystème d'Internet. En plus des utilisateurs, toutes les données y sont interconnectées de manière décentralisée. Le Web 3.0 se développe particulièrement depuis l'arrivée de la blockchain, notamment grâce à des protocoles tels que IPFS et Filecoin (FIL).

Whale / Baleine

C'est le surnom donné aux personnes possédant beaucoup de bitcoins (ou altcoins) et qui peuvent, par le simple fait d'acheter ou de vendre, faire varier le cours d'une crypto-monnaie de façon significative.

White Paper / Livre Blanc

Adapté de l'expression *white paper*, le terme livre blanc désigne un guide pratique de quelques pages consacré à la présentation d'un projet ou d'une crypto-monnaie. Les livres blancs sont surtout utilisés pour convaincre de l'intérêt d'un projet.

Zero-Knowledge Proof (ZKP)

Une Zero-Knowledge Proof (Preuve à Divulgation Nulle de Connaissance, ou ZKP), est un concept de cryptographie avancé qui permet à une partie, le prouveur (Prover), de prouver à une autre partie, le vérificateur (Verifier), qu'une certaine affirmation est vraie sans révéler aucune information autre que la véracité de l'affirmation elle-même. Cette définition technique implique plusieurs composants clés et propriétés :

- Complétude : Si l'affirmation est vraie, un prouveur honnête peut convaincre le vérificateur de cette vérité avec une probabilité élevée.
- Validité Sonique (Soundness) : Si l'affirmation est fausse, il est pratiquement impossible pour un prouveur malhonnête de tromper le vérificateur en lui faisant croire que l'affirmation est vraie.
- Zero-Knowledge : Si l'affirmation est vraie, le vérificateur n'apprend rien d'autre que le fait que l'affirmation est vraie. Le prouveur ne divulgue aucune information qui pourrait être utilisée pour déduire d'autres propriétés sur les données en questi

{