LEXIQUE

BLOCKCHAIN ET CRYPTOMONNAIES : LES DÉFINITIONS À CONNAÎTRE

Tous | # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Il y a actuellement 189 noms dans ce répertoire

2FA

2FA est un procédé d'authentification à deux facteurs, aussi appelé double authentification. La méthode consiste à utiliser une application sur votre smartphone qui augmente considérablement la sécurité de l'accès à une plateforme, un exchange ou un site d'investissement par exemple. Le principe est que cette application donne des nombres assez longs, qui changent toutes les trente ou soixante secondes et qu'il faut saisir après avoir entré son mot de passe pour avoir accès au site.

AMF

L'AMF est l'autorité des marchés financiers français. Elle réglemente, organise, et contrôle les différentes pratiques des acteurs de la place financière française et informe les investisseurs de chaque nouvelle réglementation. L'AMF intervient donc actuellement dans les questions de régulation des investissements et échanges de cryptomonnaies pour déterminer un cadre juridique clair pour ces nouveaux actifs financiers.

Ask

On voit systématiquement sur une plateforme de trading des valeurs « Ask » et « Bid ». La valeur « Ask » est le prix auquel les vendeurs souhaitent vendre une cryptomonnaie donnée.

ASIC

Un ASIC (Application Specific Integrated Circuit) est un type de circuit électronique intégrant sur une même puce l'ensemble des éléments actifs indispensables et spécifiques à un certain type de calcul bien précis (par exemple des hashes SHA 256

pour Bitcoin). L'ASIC permet une puissance de calcul très supérieure à une carte graphique GPU et est donc de plus en plus utilisé en minage pour les cryptomonnaies ayant un niveau de difficulté très élevé, comme Bitcoin ou Dash. Certaines cryptomonnaies ont fait le choix d'un algorithme « ASIC résistant » pour se prémunir de cette course à la puissance de calcul, qui pose d'importants problèmes environnementaux et centralise le minage en laissant très peu de chances aux mineurs particuliers de rentabiliser leur matériel. C'est par exemple le cas de Monero, basé sur l'algorithme CryptoNightV7.

Airdrop
Un airdrop consiste pour un projet de cryptomonnaie à distribuer des tokens gratuitement à sa communauté. Ces systèmes marketing permettent au projet de se faire connaitre en dynamisant sa communauté. Les airdrops sont en général reversés à des conditions précises : aimer une page Facebook, remplir un KYC, traduire un whitepaper, etc.

Altcoin
Un altcoin – ou "cryptomonnaie alternative" – désigne toute autre cryptomonnaie que Bitcoin.

ATH/ATL
« ATH » signifie « All time high », et désigne ainsi le prix le plus haut jamais atteint par une cryptomonnaie.« ATL » signifie à l'inverse « All time low » et désigne donc le prix le plus bas qu'elle n'ait jamais atteint.Ces deux données sont importantes pour définir des supports et résistances sur chaque cryptomonnaie.

Arbitrage
L'arbitrage consiste à profiter des différences de prix entre deux différentes plateformes d'échange, en achetant sur l'une et en revendant sur l'autre. L'arbitrage doit également tenir compte des commissions pour rester stratégique et permettre au trader de maximiser son profit.

Analyse fondamentale
L'analyse fondamentale est une méthode sur laquelle les investisseurs s'appuient pour estimer l'évolution de la valeur intrinsèque d'un bien ou un actif. L'analyse fondamentale cherche à interpréter tous les différents facteurs pouvant impacter son prix futur : événements et influences externes, éléments internes à l'entreprise (diagnostic financier, ressources humaines, etc). L'analyse fondamentale se base bien souvent sur une analyse SWOT (Forces, Faiblesses, Opportunités, Menaces). Elle doit être complétée par une analyse technique si l'on souhaite mener des activités de trading, et ce quel que soit l'actif considéré (cryptoactif, indices de bourse, Forex, etc.).

Cliquez ici pour apprendre à faire de bonnes analyses fondamentales »

Analyse technique
Une analyse technique permet d'étudier et d'anticiper les mouvements de marché à partir d'indicateurs clés. Elle repose sur l'étude des différents graphiques de l'historique d'un actif à différentes échelles de temps, ces échelles variant en fonction de la méthode de trading privilégiée (swing trading, day trading ou scalping). L'analyse technique permet de déterminer les tendances de marché pour mieux anticiper les mouvements à venir choisir de manière stratégique son point d'entrée et de sortie.

Bid
« Bid » signifie « offre » en français. On voit souvent sur une plateforme de trading des valeurs « Ask » et « Bid ». La valeur « Bid » est le prix auquel les acheteurs souhaitent acheter une cryptomonnaie donnée. À l'inverse le « Ask » renvoie au prix qu'en demandent les vendeurs.

Bloc
Un bloc est l'élément principal d'une blockchain, ou "chaîne de blocs" en Français. Chaque bloc contient un ensemble de transactions, qui, une fois intégré à la blockchain, permet au mineur de gagner une récompense. La récompense sur Bitcoin est actuellement de 12,5 bitcoins. Le délai de production d'un bloc varie en fonction des différentes cryptomonnaies. Sur Bitcoin, un bloc est intégré à la blockchain toutes les 10 minutes.

Burn
Burn, de l'anglais "brûler", est le fait de supprimer un certain nombre de tokens d'une cryptomonnaie pour faire baisser l'offre totale disponible. Concrètement, les tokens sont envoyés vers une adresse publique dont personne ne connaît la clé privée et sont donc inutilisables. Cela créé un déséquilibre entre l'offre et la demande et vise généralement à augmenter la valeur de chaque token.

Bitmex
BitMEX est une plateforme de trading de cryptomonnaies proposant des options spécifiques de *margin trading*. Son utilisation est adaptée aux traders aguerris. Il est possible d'y trader des contrats futures ou des contrats perpétuels. BitMEX propose un effet de levier allant jusqu'à X100. La plateforme ne fonctionne avec aucune monnaie fiat : les dépôts doivent donc se faire en Bitcoin.

Cliquez ici pour ouvrir un compte BitMEX et bénéficier de 10% de réduction sur vos frais pendant 6 mois grâce à notre lien affilié.

BitPay
BitPay est un système de paiement permettant aux e-commerces d'accepter les paiements en bitcoins. Il est surnommé le « Paypal de Bitcoin » et traite les paiements en Bitcoin de plus de 40 000 entreprises et organisations. Il permet la conversion instantanée en USD, EUR, GBP, CAD et beaucoup d'autres monnaies nationales, et protège ainsi les marchands du risque de volatilité du Bitcoin tout en leur permettant de diversifier les moyens de paiements acceptés.

Bearish
Bearish est un terme anglais dérivé du mot bear (ours) qui désigne l'état d'esprit d'un investisseur qui pense que la tendance est baissière. La métaphore de l'ours est utilisée pour caractériser un marché baissier en raison de la manière dont un ours combat. Celui-ci attaque son adversaire avec ses pattes avant, en donnant des coups de haut en bas.

Binance
Binance est une des principales places de marché permettant d'échanger des cryptomonnaies. L'exchange s'est financé via une ICO en 2017 avec le token Binance Coin (BNB) et est rapidement devenu la principale plateforme d'échange en termes de volume et de sécurité. Vous pouvez consulter une vidéo complète explicative destinée aux débutants pour vous y inscrire.

Bittrex
Bittrex fait également partie des principales plateforme d'échange de cryptomonnaie. Elle ne permet cependant pas d'échanger des cryptomonnaies contre des devises plus classique, comme l'euro ou le dollar.

Bullish
Bullish est un terme anglais dérivé du mot bull (taureau) qui désigne l'état d'esprit d'un investisseur qui pense que la tendance est haussière. Par extension, bullish appliqué à un marché indique que la plupart des observateurs pensent que ce marché est sur une tendance haussière.

Bitfinex
Bitfinex est la plateforme d'échange de cryptomonnaies avec le volume de transactions le plus important pour la paire BTC/USD. On retrouve fréquemment des commentaires affirmant que Bitfinex "drive le marché", signe de son importante influence. Elle a pour particularité d'intégrer l'euro et le dollar, & offre à ses utilisateurs des outils destinés aux traders expérimentés. C'est la plateforme qui permet le short selling sur le plus de paires de cryptomonnaies. Vous devez disposer d'un capital de minimum 10 000 $ pour ouvrir un compte sur la plateforme.

Bear trap
Bear trap signifie en français “piège baissier”. Cela caractérise une situation dans laquelle un investisseur ou un trader vend à découvert une position, en anticipant une baisse du marché à partir d’un faux signal de vente. La tendance ne se retourne donc pas à la baisse comme prévu, mais poursuit sa hausse. Le trader ou l’investisseur est donc forcé de racheter son actif plus cher que ce qu’il ne l’a vendu pour clôturer sa position rapidement.

Bandes de Bollinger
Les bandes de Bollinger est un outil de trading développé par John Bollinger. Cet indicateur réalise une mesure dynamique de deux éléments : la volatilité et la directionnalité du prix. Lorsqu’il y a une augmentation de la volatilité et une forte directionnalité, le prix sort des bandes. Il s’agit d’un événement rare puisque statistiquement, le prix ne sort des bandes qu’environ 5 % du temps.

Binance Coin (BNB)
BNB est la cryptomonnaie vendue lors de l’ICO de Binance. Elle sert à payer des frais de transaction sur la plateforme d’échange. En payant en BNB, les frais de transactions sont réduis de 50%. Le Binance Coin (BNB) ne se trouve que sur la place de marché de Binance.

Block lattice
Le block lattice est une technologie de DLT proposant une structure novatrice de blocs, utilisée pour la première fois par la cryptomonnaie Raiblocks (rebaptisée Nano). Il s’agit de blocs tressés permettant à chaque compte utilisateur de disposer de sa propre chaîne de blocs stockant le solde et l’historique des transactions. Le propriétaire du compte-chaîne est le seul à pouvoir mettre celui-ci à jour. Le block lattice est une solution idéale pour les micropaiements, car elle permet des transactions instantanées et sans frais, tout en pouvant gérer un très grand nombre de transactions simultanément.

Blockchain
La blockchain est un type de **technologie de registres distribués** (*distributed ledger technologies* en anglais, ou DLT). Elle se présente comme une grande base de données formée de blocs, liés les uns aux autres de manière cryptographique, contenant des informations (transactions, lignes de codes etc.). Ces blocs sont ajoutés selon un protocole très précis et consultable par tous. La particularité de la blockchain est qu’elle est par essence décentralisée, car chacun peut y contribuer en formant des blocs qui sont ajoutés à celle-ci, selon certaines conditions très strictes définies par un **protocole de consensus**. Les cryptomonnaies sont la première application viable de la technologie de la blockchain. Le web décentralisé pourrait être la suivante. On distingue par ailleurs blockchains publiques et privées : chez la première, chacun peut

participer à la continuation de la blockchain, chez la seconde les participants sont choisis selon certains critères par le créateur de la blockchain.

Allez plus loin avec la formation “Blockchain et cas d’usage” de BitConseil »

Bulle spéculative

Une bulle spéculative est une progression démesurée du cours d’un titre, d’un indice, voire d’un secteur tout entier. Cette hausse est décorrélée de la croissance réelle du marché ou d’une économie. La formation d’une bulle est provoquée par un excès de spéculations optimistes sur la croissance des valorisations. Une bulle peut perdurer plusieurs mois ou plusieurs années avant d’éclater. L’éclatement d’une bulle est suivi par une baisse drastique des cours qui provoque ce que l’on appelle communément un « krach ».

CFD

Un CFD (Contract for difference) est un instrument financier (un produit dérivé) permettant de parier sur la hausse ou la baisse du cours d’un actif financier, sans acheter directement cet actif.Prenons l’exemple d’un CFD à l’achat sur Bitcoin. Un contrat est passé entre l’acheteur et le vendeur. Si le prix de Bitcoin monte, votre position sera positive. Si vous clôturez votre position à ce moment là, alors le vendeur du CFD vous devra la différence entre le prix d’achat et le prix de revente. Si au contraire vous clôturez votre position à un prix inférieur à votre entrée en position, c’est vous qui devez de l’argent au vendeur. Vous êtes en perte.Il est possible de vérifier si l’on a acheté un CFD ou la cryptomonnaie en essayant de la transférer sur le portefeuille numérique adapté. Si le transfert ne se fait pas, c’est qu’il s’agit d’un CFD. Nous recommandons vivement de vous éloigner de ce type de produit financier si vous n’êtes pas expérimenté.

CPU

Le CPU (pour Central Processing Unit, soit Unité Centrale de Traitement) est l’organe central d’un ordinateur. Un CPU est un processeur ou microprocesseur et contient tous les circuits logiques permettant d’exécuter un programme. Dans le monde des cryptomonnaies, on distingue le minage sur CPU, qui réclame peu de puissance de calcul, du minage sur GPU (carte graphique) et enfin de l’ASIC, qui permet une puissance de calcul bien supérieure.

Coin

Coin, de l’anglais “pièce”, est le mot couramment utilisé pour décrire l’unité comptable d’une cryptomonnaie. On distingue les coins des tokens. Un coin fait référence à une cryptomonnaie servant d’unité de compte, réserve de valeur et intermédiaire des échanges. Un token désigne une cryptomonnaie donnant accès à un droit ou à un service particulier sur une DLT publique. Notons qu’une seule et même cryptomonnaie peut être à la fois un coin et un token.

Casper
Casper est une mise à jour très attendue du protocole de consensus Ethereum, qui prévoit en 2019 son passage d'un mécanisme de PoW (Proof of Work) à un mécanisme de PoS (Proof of Stake). Lors du lancement de Casper, Ethereum utilisera temporairement un mécanisme hybride entre le PoW et le PoS puis finira par utiliser seulement le PoS dans une mise à jour ultérieure.

Coinbase
Coinbase est l'une des plus grandes plateformes d'achat de cryptomonnaies. Il s'agit certainement de la meilleure plateforme où acheter des bitcoins pour débuter dans le monde des cryptomonnaies. Coinbase est d'autant plus pratique qu'il est possible d'y acheter des bitcoins par carte bancaire, en plus des paiements par virement SEPA.

Courtier
Un courtier (broker en anglais) est un intermédiaire indépendant qui vous propose de vendre ou acheter des actifs et se rémunère en prenant une commission. Vous pouvez faire appel à un courtier soit car il est habilité à intervenir sur un marché donné, soit pour sa capacité à faire fructifier un capital.

Consensus
Le consensus n'est pas un terme propre aux cryptomonnaies, mais il est un élément essentiel au bon fonctionnement de tout système. Le consensus est la vérité admise par les participants au système. Cela ne veut pas dire que le consensus est la vérité absolue ou qu'il est incontestable, mais c'est la réalité sur laquelle s'accordent les participants au système. Dans le sport par exemple, c'est l'arbitre qui crée le consensus en cas de désaccord. Dans le monde judiciaire, c'est le juge. Dans le monde des cryptomonnaies, divers algorithmes, commençant par "Proof of XXXXX" permettent de parvenir au consensus sur une blockchain. La force d'une blockchain est dès lors de parvenir systématiquement, efficacement et de manière décentralisée à un consensus : on parle de "protocole de consensus" ou de "mécanisme de consensus".

Chandeliers japonais
Les chandeliers japonais sont une forme de représentation du comportement du prix en fonction de l'unité de temps que l'on a sélectionné. Il est généralement vert si le prix a évolué à la hausse, et rouge si le prix a évolué à la baisse. Pour plus d'information, vous pouvez consulter cette vidéo du Trading Du Coin.

Coin Stats
Coin Stats est la première application portfolio de Bitcoin et d'altcoins permettant de suivre en temps réel les cours des cryptomonnaies sur plus de 100 plateformes

d'échange. L'application peut être automatiquement synchronisée à des wallets et comptes d'exchange et permettre à chaque investisseur de connaître la valeur de son portefeuille sans avoir à ajouter manuellement ses transactions. Il est également possible de paramétrer des alertes pour être averti quand le cours d'une cryptomonnaie atteint un certain niveau.

CoinMarketCap.com
CoinMarketCap est un site de référence du marché des cryptomonnaies. Il contient une liste très importante de cryptomonnaies et permet d'être informé sur plusieurs informations essentielles sur celles-ci : prix, place de marché sur laquelle l'actif est listé, lien vers le whitepaper, volume de transactions en fonction des exchanges...

Cold storage
Le cold storage – ou "stockage à froid" – désigne une manière de détenir et de stocker ses clés privées sur un support déconnecté d'Internet. Il est possible de stocker ses clés privées sur une simple feuille de papier – un paper wallet – ou d'utiliser des portefeuilles électroniques comme le Ledger Wallet ou le Cool Wallet.

Contrat intelligent / Smart Contract
Un contrat intelligent (smart contract en anglais) est un protocole informatique du type "s'il se passe ceci, alors cela se produit et inversement". En anglais, on y fait référence avec l'expression "if-then". Un contrat intelligent peut être exécuté automatiquement via des outils numériques, pourvu que ceux-ci puissent puiser les données nécessaires au fonctionnement du contrat. Les outils numériques permettent en effet de vérifier en temps réel si les conditions du contrat sont respectées et si l'heure est venue pour qu'un événement en particulier se produise. Des Oracles peuvent entrer en jeu pour fournir des données au système que des machines ne peuvent pas constater dans le monde réel ou évaluer convenablement. Voir la définition "smart contract" complète ici.

Correction
Une correction est un retournement rapide et brutal du cours d'une cryptomonnaie, à la hausse ou la baisse. On parle de « correction » car suite à ce retournement, le prix se rapproche de son cours précédent, après une période de hausse ou de baisse plutôt longue.

Cryptoactif
En 2018, les cryptomonnaies ont été requalifiées par l'AMF, qui leur préfère désormais le terme de « cryptoactif ». Ce terme représente mieux le sous-jacent de la majorité des cryptomonnaies, qui sont plus facilement assimilables à des actifs financiers qu'à des monnaies traditionnelles ayant pour fonction l'unité de compte, la réserve de valeur et l'intermédiaire d'échanges.

Cryptomonnaie
Une cryptomonnaie est une monnaie numérique basée sur les principes de la cryptographie. Elle s'échange sur un réseau décentralisé, en pair à pair, grâce aux technologies de Distributed Ledger Technologies (DLT) comme la blockchain, les DAG ou le block lattice. Elle intègre l'utilisateur dans les processus de stockage, d'émission et de règlement des transactions et supprime l'intervention d'un intermédiaire ou d'un tiers de confiance comme une banque.

DAG
Un DAG (Direct Acyclic Graph, ou Graphe Orienté Acyclique en français) est un type de **technologie de registres distribués** (DLT), tout comme la blockchain. Les technologies de DAG n'ont pas recours aux blocs, mais utilisent un graphe acyclique direct où les informations sont stockées dans des noeuds. Les transactions sont liées les unes aux autres : une transaction confirme la suivante et ainsi de suite. Les DAG ont l'avantage d'être plus scalables que les blockchains, plus rapides et plus adaptés aux microtransactions. Mais ces réseaux sont également plus vulnérables face aux attaques. Les cryptomonnaies les plus connues à être basées sur un DAG sont IOTA et ByteBall.

DAO
Une DAO est une Decentralized Autonomous Organization, autrement dit une organisation décentralisée autonome, ce qui signifie que ses règles de gouvernance sont entièrement automatisées et ne requièrent en principe aucune intervention humaine. La DAO repose donc sur un principe "trustless" (sans confiance), qui supprime la nécessité d'accorder sa confiance à un tiers : dans une DAO, « code is law », autrement dit le code fait la loi. Les règles de fonctionnement d'une DAO sont inscrites dans une blockchain et sont donc à la fois immuables et transparentes.

Dip
Un dip est une chute brutale, mais éphémère du cours d'une cryptomonnaie. Après un dip, une cryptomonnaie retrouve très rapidement sa valeur. Un dip peut résulter de différents mécanismes de marché, très souvent il s'agit d'une vente de la part d'un poids lourd (une « baleine » ou un « whale », selon le jargon du marché crypto). L'idéal est de parvenir à acheter une cryptomonnaie pendant un dip pour réaliser une belle plus-value.

DLT
Une DLT (Distributed Ledger Technology) est une technologie de registres distribués. Le but d'une DLT est d'améliorer la transparence, la sécurité et la traçabilité des informations liées à différentes transactions en partageant un registre immuable et consultable par tous. Les DLTs peuvent être publiques ou privées, et restreindre ainsi l'accès à une minorité de personnes autorisées. La quasi-totalité des cryptomonnaies

du marché actuel sont basées sur des DLTs publiques. Une grande majorité d'entre elles sont basées sur des blockchains, toutefois la blockchain n'est pas le seul type de DLT possible : il existe également des technologies comme le DAG (Direct Acyclic Graph), utilisé par IOTA sous forme de *tangle*, ou le *block lattice*, utilisé par Nano.

DApp

DApp est un acronyme anglais signifiant "decentralized application" (application décentralisée). Une application décentralisée fonctionne sur un réseau d'ordinateurs appelé souvent virtual machine, comme l'EVM (Ethereum virtual machine), ce qui lui permet d'être "indestructible" car disséminée sur plusieurs ordinateurs plutôt que sur un serveur d'Amazon, Google ou Microsoft. Des réseaux comme Ethereum, Stratis ou EOS sont dédiés à l'hébergement de ces DApps. Voir la définition DAPP complète ici.

DDoS

Une attaque DDoS (attaque par déni de service, Denial of Service) vise à rendre inaccessible ou inopérant un système informatique pendant une certaine durée. Ce type d'attaque ouvre la voie aux hacks (piratages) et à des vols importants sur les plateformes d'échange de cryptomonnaie. Chaque jour, les exchanges sont victimes de tentatives d'attaques DDos et doivent donc savoir s'en protéger pour continuer à résister aux attaques et protéger leurs fonds.

DPOS

Le protocole DPOS, pour Delegated Proof of Stake, est un algorithme de consensus blockchain développé par Daniel Larimer et utilisé pour la première fois pour la blockchain BitShares. Le protocole DPOS consiste en une preuve d'enjeu déléguée qui vise à résoudre les problèmes de centralisation que posent les mécanismes de Proof of Work et Proof of Stake.Chaque utilisateur du réseau détient un droit de vote proportionnel à ses possessions de tokens en vue d'élire différents délégués. Seuls les délégués pourront contribuer à la production des blocs, mais les membres du réseau ont le dernier mot sur toutes les modifications effectuées sur le protocole. Le système est parfois critiqué pour les abus de position dominante des délégués, qui peuvent rester en place très longtemps. D'autres part, plus le nombre de délégués est faible, plus la centralisation est importante (21 pour EOS, 51 pour Ark, 101 pour Lisk).

Dump

Un dump consiste tout simplement en la baisse du prix d'une cryptomonnaie. Un dump est généralement une baisse prolongée, qui peut susciter de l'inquiétude chez les traders ou les investisseurs.

Dust

Le dust, poussière en français, correspond à tous ces faibles montants de cryptomonnaies que l'on conserve dans son wallet si l'on fait régulièrement du

trading, et que l'on ne peut ni vendre ni convertir, les montants étant trop bas. Chez Binance, il est possible de convertir ses dusts en BNB (token de la plateforme) pour les récupérer ou payer des frais de transaction avec.

DYOR

DYOR est l'acronyme de "Do Your Own Research", soit en Français, "faites vos propres recherches". C'est un adage très courant en finance qui est souvent répété aux novices. Il faut toujours effectuer ses propres recherches avant de réaliser quelconque investissement.

Pour l'anecdote, le directeur de la CFTC aux États-Unis, Christopher Giancarlo (que l'on sait favorable aux cryptomonnaies) était sorti d'une session au Sénat sur la thématique des cryptomonnaies en écrivant sur Twitter "Merci pour votre énorme réponse à mes récentes remarques au Sénat US. Lol. En investissant, rappelez-vous : soyez prudent, mesuré et DYOR".

https://twitter.com/giancarloMKTS/status/961612907732783104

Déflation

La déflation s'oppose à l'inflation, et désigne donc la baisse des prix. Elle est souvent confondue avec une baisse de l'inflation – la désinflation – qui consiste en une diminution de la hausse des prix, et non en une baisse. . La déflation est synonyme de régression d'un marché ou d'une économie, si bien que l'on parle souvent de « spirale déflationniste ». Il n'est donc pas souhaitable d'observer une situation de déflation sur le marché des cryptomonnaies, pas plus que sur n'importe quel autre marché monétaire.

Downtrend

Downtrend désigne simplement une tendance baissière, ce qui est sa traduction en français.

Daniel Larimer

Daniel Larimer est à la fois développeur et entrepreneur dans le domaine des cryptomonnaies. Créateur de BitShares en 2014 , cofondateur de la blockchain Steemit en 2016, et directeur technique de la société Block.one (projet EOS), Dan Larimer est une des principales figures de l'écosystème des cryptomonnaies et est très reconnu par la communauté crypto. Il est également à l'origine du premier algorithme de consensus DPOS (Delegated Proof of Stake), depuis repris par de gros projets comme Lisk.

Day Trading

Le day trading consiste à prendre des positions de trading plutôt courtes, allant de quelques heures à quelques jours maximum. Le day trading requièrt une disponibilité importante pour pouvoir chaque jour surveiller ses positions et profiter des hausses ou des baisses des cours. Le day trading se distingue du swing trading (échelle de temps plus longue) et du scalping (échelle de temps plus courte).

Difficulty Target

Dans le système Proof of work, la difficulty target, “niveau de difficulté” en français, est une condition que doit remplir le hash d’un bloc pour que celui-ci soit accepté par le réseau et que le mineur qui a créé ce bloc empoche sa récompense. Sur Bitcoin par exemple, la difficulty target actuelle exige que le hash commence par vingt zéros, ce qui est extrêmement difficile à atteindre et demande des consommations d’énergie très importantes.Le niveau de difficulté varie au cours du temps pour que la fréquence de création des blocs soit conforme à celle indiquée dans le protocole de la cryptomonnaie. Plus le niveau de difficulté est élevé, plus les mineurs doivent « travailler » pour le satisfaire, valider un nouveau bloc et toucher la récompense correspondante. Plus il y a de mineurs, plus la difficulté doit être réajustée à la hausse pour que la fréquence de création de blocs reste constante, comme c’est le cas notamment de Bitcoin où le niveau de difficulté est ajusté (réhaussé) tous les 2016 blocs, soit environ deux semaines.

Double spending

Le double spending, la double dépense en français, est précisément une des innovations de Bitcoin, proposé par Satoshi Nakamoto fin 2008. Comme son nom l’indique, la double dépense consiste à dépenser deux fois le même jeton.C’est le problème majeur des actifs numériques, qui, par définition, ne sont que du code informatique. La duplication de fichiers informatiques a notamment était un grand problème dans l’industrie de la musique. Cela a permis de partager des fichiers illégalement sur Internet.Bitcoin résout le problème grâce au système cryptographique qu’est sa blockchain décentralisée. Si les mineurs reçoivent deux transactions dépensant les mêmes bitcoins, ils n’acceptent que la première transaction et refusent la seconde.

ERC-20

L’ERC-20 (Ethereum request for comment n°20), est un contrat intelligent standard qui permet la création de tokens basés sur la blockchain Ethereum, autrement dit sans devoir développer une nouvelle blockchain. C’est l’outil majeur utilisé par les organisateurs d’ICO qui leur permet de créer une nouvelle monnaie en s’appuyant sur l’efficacité et la bonne réputation de la blockchain Ethereum.

Exchange

Une plateforme d’échange, ou un exchange en anglais, est une place de marché dédiée aux cryptomonnaies. Outre la possibilité de vendre et d’acheter des

cryptomonnaies et éventuellement des monnaies fiat, les exchanges mettent à votre disposition un wallet qui vous permet de stocker, de transférer vos coins, et d'en recevoir venant d'autres personnes. Il est à noter que c'est l'exchange qui contrôle la clé privée du portefeuille dans ce cas, pas vous. Il existe actuellement plus de 10 000 plateformes d'échanges de cryptomonnaies plus ou moins grandes, sécurisées, et spécialisées sur certaines monnaies. Chaque plateforme se rémunère en prélevant des frais, généralement peu élevés (presque toujours en dessous de 1%), sur chaque opération, sauf le stockage de monnaie, qui est gratuit.

Échange décentralisé

Les plateformes d'échanges décentralisées, ou DEXs pour Decentralized Exchanges, proposent une alternative aux grosses plateformes d'échange centralisées comme Binance, Bittrex ou Kraken pour permettre aux utilisateurs d'échanger leurs cryptomonnaies sur des marchés de pair à pair directement sur la blockchain. Les traders restent ainsi dépositaires de leurs fonds et évitent les risques de piratage qui peuvent subvenir sur des plateformes d'échange centralisées. Les DEX permettent ainsi de se passer entièrement de tiers de confiance pour profiter pleinement des avantages de la blockchain. L'utilisation de ces plateformes est cependant complexe et très peu intuitive.

Effet de levier

L'effet de levier permet de multiplier son exposition sur le marché, tout en n'immobilisant qu'une partie de son capital, que l'on appelle la couverture. Le courtier met à disposition la partie restante de la valeur totale de la position. Les gains et les pertes sont calculés sur la valeur totale de la position. L'effet de levier permet de gagner de très importantes sommes, mais expose également à des risques proportionnels de perte. L'effet de levier existe pour la pluspart des produits financiers, y compris les cryptomonnaies. Trader avec un effet de levier est possible sur BitMEX.

Equity token

Un equity token donne à son investisseur des droits en contrepartie des fonds apportés à une entreprise, au moment de son ICO ou ultérieurement. Un equity token fonctionne selon le même principe qu'une action : il représente une participation au capital de l'entreprise et permet donc de toucher d'éventuels dividendes. L'augmentation de sa valeur est corrélée à celle de la valeur produite par l'entreprise. Il existe d'autres types de tokens, comme les security ou les utility tokens.

Étoile du soir

L'étoile du soir est une figure graphique de 3 chandeliers japonais annonçant un retournement baissier du marché :Une première bougie haussière avec un grand corps ;Une deuxième bougie d'indécision (grandes mèches et petit corps) ;Une troisième bougie baissière avec un grand corps.

FUD
Fear, uncertainty and doubt (peur, incertitude et doute). Le FUD est une technique utilisée en marketing. Dans les cryptomonnaies, le FUD consiste à tenter d'influencer d'éventuels investisseurs ou traders en diffusant des informations négatives suffisamment vagues pour semer le doute. Le FUD consiste par exemple à dénigrer une crypto-monnaie ou un projet.

Fiat
Fiat est un mot d'origine latine qui n'a rien à voir avec le constructeur automobile et qui est le synonyme de fiduciaire. Fiat signifie "qu'il soit ainsi" en latin et désigne une monnaie qui a un cours légal et imposé par l'émetteur, qui peut être un État ou un groupe d'États (dans le cas de l'euro), comme l'euro, le yen ou le dollar US.

FOMO
FOMO est l'acronyme anglais de Fear of Missing Out. Sur les marchés financiers, cette expression désigne la peur d'un investisseur ou d'un trader de manquer une bonne affaire, qui pousse à agir de manière impulsive pour être sûr de prendre le train en marche. Le FOMO est étroitement lié à la psychologie des foules et est très courant sur le marché des cryptomonnaies, qui comporte un grand nombre d'investisseurs ou de traders peu familiers avec les mouvements de marché.

Fork
Un fork, bifurcation en français, est la mise à jour du programme qui régit une blockchain. Si cette mise à jour modifie les règles de consensus, mais que ces nouvelles règles restent compatibles avec les précédentes, on parle de soft fork. Par analogie logicielle, un soft fork peut être comparé à une mise à jour Windows pour rendre le système plus sûr.Si en revanche les nouvelles règles de consensus induisent un tel changement qu'elles sont incompatibles avec les précédentes, un nouvel exemplaire de la blockchain est créé et on parle alors de hard fork. Une des deux blockchain appliquera dans ce cas les nouvelles règles, l'autre continuera à appliquer les anciennes.

Faucet
Un faucet, robinet en anglais, est un site ou une partie d'un site où l'on peut, en effectuant des actions très simples comme cliquer sur un bouton, récupérer des parties infinitésimales de cryptomonnaies.

Forgeur
Un forgeur peut être assimilé à un mineur, sauf que celui-ci contribue au protocole d'une blockchain basée sur un mécanisme de Proof of Stake, et non de Proof of Work. Un forgeur est donc une personne qui participe à la création des blocs d'une blockchain PoS. Celui-ci est choisi par l'algorithme de manière aléatoire pour forger le

prochain bloc de la chaîne. Plus un forgeur possède de tokens de la blockchain en question, plus celui-ci a de chances d'être sélectionné pour forger le prochain bloc. Il sera ensuite rémunéré pour chaque bloc qu'il sera parvenu à forger et valider.

Futures
Les "Futures", ou contrats à terme, sont des produits dérivés d'actifs sous-jacents prenant la forme de contrats dûemment approuvées par les autorités de régulation. Un future peut porter sur tout type de sous-jacent : or, matières premières, et depuis peu, les cryptomonnaies. Vous pouvez par exemple trader Bitcoin sur Futures en allant sur BitMEX.

L'intérêt d'utiliser des contrats futures au lieu d'acheter directement une cryptomonnaie se trouve principalement chez *hodleurs*. EN cas de marché baissier, il peuvent laisser leurs cryptomonnaies dans leur haldware wallet, et prendre une position courte – *à la baisse* – sur les futures. Cela leur permet de se protéger contre la baisse du prix de leurs actifs.

Futarchy
Le terme anglais futarchy, qui n'a pas encore de traduction officielle en français, désigne une forme de gouvernement dans laquelle les marchés prédictifs sont utilisés pour déterminer quels choix politiques seront faits.

Flippening
Le flippening désigne le moment où la capitalisation totale d'Ethereum (ETH) dépassera celle de Bitcoin (BTC)."The flippening" est une théorie née suite à l'envol du prix d'Ethereum (ETH) et à la diminution de la Dominance de Bitcoin. Ce phénomène a failli avoir lieu en juin 2017. La capitalisation d'Ethereum était de 37 milliards de dollars et celle de Bitcoin s'élevait à 45 milliards de dollars.Depuis, ce terme peut désigner d'autres luttes pour une position sur le marché entre deux cryptomonnaies. Ethereum a par exemple perdu sa deuxième place au profit de Ripple en décembre 2017, pour la reprendre en janvier. Cette théorie est souvent moquée sur les réseaux et est représentée par un dauphin tournant en rond.

Gas
Certaines blockchains de smart contracts, comme Neo ou Ethereum, utilisent plusieurs tokens, dont le *gas*. Sur ces blockchains, le gas est utilisé pour payer les frais de transactions ou exécuter les différentes opérations prévues par un smart contract. Pour utiliser la blockchain Ethereum ou Neo, il est donc indispensable de posséder du gas. Dans le cas de Neo, il est possible de miner du Gas directement depuis son wallet.

GPU

Un GPU (Graphical Processing Unit) est un processeur des cartes graphiques équipant les ordinateurs. Les GPU sont optimisés pour les calculs et sont donc beaucoup utilisés pour le minage de cryptomonnaies. Les rigs de minage sont composés de plusieurs cartes graphiques pour maximiser la puissance de calcul. Une ferme de minage contient plusieurs centaines de GPU. Pour certaines monnaies, le minage par GPU s'avère insuffisamment puissant et les ASIC sont désormais indispensables pour s'appuyer sur une puissance de calcul supérieure.

Gestion des risques

La gestion des risques est indispensable pour tout trader. Il s'agit d'un ensemble de règles à appliquer au cours de son activité pour contrôler les risques afin de protéger son capital, et d'augmenter ses bénéfices. En trading, la gestion du risque est essentielle pour limiter ses pertes. Maintenir une bonne gestion du risque implique de savoir garder la tête froide pour gérer ses émotions.

Hack

Un hack est un piratage informatique. Dans le monde des cryptomonnaies, un hack peut consister à dérober des mots de passe privés sur un exchange, à exploiter une faille de l'algorithme de consensus en effectuant des doubles-dépenses, ou à mener une attaque des 51% pour s'attribuer illégalement des coins, comme ce fut le cas en mai 2018 chez Verge ou Bitcoin Gold.

Hash

Le hash (terme anglais) peut être traduit en français par « somme de contrôle » ou « empreinte ». Le hash est utilisé en informatique, mais aussi en cryptographie. Une empreinte vise à authentifier une donnée initiale (parfois inconnue), en pouvant la comparer avec d'autres empreintes.En cryptographie, l'empreinte est le résultat de l'application d'un logiciel de chiffrement à un message donné. Quelle que soit la nature des données entrées dans le logiciel de chiffrement, l'empreinte aura toujours la même syntaxe, c'est à dire le même nombre et le même type de caractères. Par exemple, si j'applique un logiciel imaginaire de chiffrement aux formules « New York » suivies de nombres aléatoires, j'obtiens les hashes (empreintes) à droite de la flèche qui sont une série de lettres et chiffres inintelligibles mais toujours de mêmes longueur et format :"New York0" → 2fa8bc6ea3b7d1754f5ccb4a924f9aa7a83ff430e57bb7"New York1" → 203eefcbcf1e5c0d10b487ebe976f63b6285eda1f99432"New York2" → c67d4d115d57752899af1c2bc61b1073d938f8fd9907cc"New York67789" → c042b08c9af9465e41d0cf4bba0b16d810b0e04098178f"New York67790" → 98ed5f89492a32440f159fac05b642e1fe3c84ca1dab86"New York67791" → 13b357ff4c15b935694a51042b923527cc88b739a58f74

Hodl

Le mot « Hodl » est fréquemment employé sur les forums crypto. Ce mot vient en réalité du mot « hold », qui signifie en anglais maintenir, conserver. L'utilisation de « hodl » viendrait du fait qu'il y a plusieurs années, une personne ivre ait posté sur BitcoinTalk un message pour inciter les investisseurs à ne pas paniquer et à ne pas vendre malgré la chute des prix : au lieu d'écrire « hold », celui-ci aurait écrit « hodl ». Le terme est depuis resté et continue à être employé à chaque dump d'une cryptomonnaie pour empêcher les différents investisseurs de céder à la panique.

Hold
Le terme « hold » (du français tenir, conserver) continue d'être utilisé sur les forums pour inciter les crypto-investisseurs à ne pas vendre en tendance baissière et à patienter jusqu'à la remontée des cours pour éviter les chutes de cours trop violentes. Le marché des cryptomonnaies est encore très sensible à la psychologie des foules et la panique peut s'installer rapidement en cas de retournement d'une tendance. Inciter les investisseurs à « hold » vise donc également à faire doucement mûrir le marché pour éviter une volatilité extrême. On notera cependant que ce terme n'est pas spécifique au marché des cryptomonnaies, mais reste un reste généraliste pour les marchés.

Hacker
Un hacker est un pirate informatique.

Hacking
Le hacking est l'activité de piratage informatique.

Hard cap
Le Hard Cap d'une ICO est le budget maximal que l'entreprise ou l'association prévoit de lever. Il est ainsi considéré que tous les fonds supplémentaires au hard cap seront a priori inutiles par rapport au maximum de jetons de prévus. Selon la nature du token distribué lors d'une ICO (equity, security ou utility), le hard cap peut sensiblement varier. Bien entendu, celui-ci dépend également du niveau d'avancement, de la complexité et de l'envergure du projet, qui nécessite plus ou moins de fonds.

Hash rate
Le hash rate est le taux de hashage par unité de temps. L'unité de temps utilisée est le H/s (hashes/seconde). Dans le cas de bitcoin, nous en sommes au PH/s (1 million de milliard de hashes par seconde).

Hardware wallet
Un *hardware wallet* est la manière la plus sécurisée de stocker ses cryptomonnaies. Le hardware wallet est un portefeuille physique qui permet un

stockage à froid. Il se distingue ainsi des wallets en ligne ou *desktops wallets*, beaucoup moins sécurisés et plus facilement piratables. La particularité d'un hardware wallet est de protéger entièrement l'accès à la clé privée de son utilisateur (nécessaire pour accéder aux fonds du portefeuille). Le propriétaire lui-même n'a pas connaissance de sa clé privée : un code et une clé de récupération lui permettent d'y accéder, sans que celui-ci ne puisse la lire. Les hardware wallets les plus connus sont le Ledger Nano X, le Ledger Blue, le Trezor, et le Cool Wallet S.

Hot Storage
Par opposition au cold storage, le hot storage est le fait de stocker ses clés privées et autres mots de passe sur un périphérique connecté ou carrément en ligne. Les desktop et exchange wallets sont par essence du hot storage, tandis que les hardware wallets et paper wallets sont du cold storage.

Hyperledger
Hyperledger est une blockchain privée (ou blockchain de consortium) soutenue par la Fondation Linux. Hyperledger est open source et est sans doute la blockchain privée la plus complète du marché, car elle offre de nombreuses possibilités aux entreprises. Elle est également l'une des plus complexes à déployer. Hyperledger est particulièrement modulable et permet de personnaliser les consensus et droits d'accès au registre. IBM a fait d'Hyperledger la base de son offre blockchain, et participe à développer différents projets aux côtés d'Airbus, JP Morgan, Intel et Cisco. Hyperledger est certainement la blockchain privée la plus utilisée avec Quorum, Corda, et Ripple dans le monde de la finance.

ICO
Une **ICO (Initial coin offering, ou Offre initiale de jeton en français)** est une levée de fonds en cryptomonnaies. Lors d'une ICO, une nouvelle cryptomonnaie est créée, et le public est invité à investir dans ce nouveau token avec généralement des ETH, mais cela peut aussi être des bitcoins ou autres monnaies "sûres". L'investisseur prend donc le risque de céder des monnaies de référence contre une monnaie qui n'existe pas encore et qui n'existera peut être jamais. Nombreuses sont les arnaques parmi les ICO. La France travaille actuellement sur la définition d'un cadre juridique pour les ICO. Pour en savoir plus, nous avons réalisé une vidéo sur les ***Initial Coin Offering***.

Joseph Poon
Joseph Poon est co-auteur du white paper et co-créateur du Lightning Network. Le Lightning Network est une avancée majeure permettant au réseau Bitcoin de gagner en scalabilité et en rapidité, et de diminuer considérablement les frais de transaction. Depuis août 2017, Poon travaille sur le projet Plasma avec Vitalik Buterin, fondateur d'Ethereum. Le projet Plasma vise à améliorer la scalabilité d'Ethereum. La solution Plasma a été implémentée pour la première fois sur une partie du réseau OmiseGo en 2017.

KYC
KYC est un acronyme renvoyant à l'expression anglaise "Know Your Customer", soit en Français "Connaissez votre client". Ce terme renvoi à toutes les procédures qui vous demandent d'envoyer des documents pour prouver votre identité. Les plateformes d'échanges par exemple, vous demanderont systématiquement de passer par une procédure de vérification KYC où vous devrez envoyer un selfie, une pièce d'identité et une preuve de résidence. Ces démarches visent à lutter contre le blanchiment d'argent. C'est une obligation légale.

Kraken
Discret mais influent et présent depuis longtemps (mi 2011) dans le monde des cryptomonnaies, Kraken est l'un des grands exchanges utilisés sur le marché. Connu pour avoir repris l'affaire Mt Gox et pour accepter beaucoup de monnaies fiat, il propose uniquement une trentaine de monnaies, parmi les plus importantes, contrairement à Binance, ou Poloniex, qui cotent beaucoup d'altcoins. Kraken représente selon certains la meilleure porte d'entrée dans le marché des cryptomonnaies, notamment en Europe car c'est le premier exchange en termes de volumes sur la paire BTC/EUR.

Lambo
Le mot « Lambo » revient parfois sorti de son contexte sur certains forums crypto. Les investisseurs l'utilisent pour faire référence à leur future voiture (la « Lambo », autrement dit la Lamborghini) une fois que leur portefeuille de cryptomonnaies leur aura permis de faire fortune. Le terme est utilisé avec humour, puisqu'aucun investisseur en cryptomonnaie ne peut avoir la certitude de voir un cours augmenter sur le long terme.

Limit
Un ordre limit est un type d'ordre de bourse utilisé également dans les marchés de cryptomonnaies où vous acceptez d'acheter ou de vendre un actif lorsque celui ci a atteint un certain prix que vous précisez. Si vous voulez acheter, l'exchange passera l'ordre lorsque l'actif aura atteint le prix que vous avez précisé à la baisse (le cours de l'actif était donc plus haut lorsque vous avez passé l'ordre limite). Si vous voulez vendre, il le fera lorsque l'actif aura atteint le prix que vous avez précisé à la hausse (le cours de l'actif était donc plus bas quand vous avez passé l'ordre limite).

Ledger
Ledger est une start-up française proposant plusieurs hardware wallets et solutions de stockage sécurisé comme Ledger Vault. Son produit phare reste le Ledger Nano S, plus populaire des hardware wallets du marché. Les clés Ledger sont actuellement au nombre de trois : Ledger Nano S, Ledger Blue et le dernier en date, le Ledger nano X. Les hardware wallets Ledger sont réputés pour proposer le meilleur rapport qualité

prix du marché. Lancée seulement en 2014, Ledger possède aujourd'hui plus de 150 salariés et fait partie des start-ups françaises à la plus forte croissance ces dernières années.

Liquid
Liquid est un projet de chaine parallèle (sidechain) sur Bitcoin (BTC) développé par Blockstream. Celle-ci permettra d'échanger des bitcoins de manière anonyme, mais également tout autre type de données : devises fiats, informations, données quelconques, etc. Le premier bloc a été produit le 27 septembre 2018.

Le consensus est obtenu d'une manière particulière puisqu'il n'y a pas de mineurs, mais 23 "fédérateurs" dont beaucoup d'exchanges. Pour en apprendre plus, nous vous invitons à lire l'article suivant : Liquid Network : une blockchain secondaire pour Bitcoin (BTC)

Liquidité
La liquidité est un indicateur important des marchés financiers qui décrit la capacité à acheter ou vendre des actifs rapidement sur une place de marché donnée sans que cela ait d'effet majeur sur les prix. Plus un marché est liquide, plus vous pouvez effectuer facilement et rapidement des transactions sur ce marché. La liquidité est une caractéristique essentielle que doit fournir un bon marché. Elle dépend notamment du nombre d'acheteurs et de vendeurs, des frais de transaction et des modalités de passage d'ordre sur ce marché.

Lightning Network
Le Lightning Network (Réseau Éclair) est une couche secondaire du protocole Bitcoin. Celui-ci vise entre autres à améliorer considérablement la scalabilité du réseau Bitcoin pour résoudre les problèmes d'engorgement lors des montées en charge. L'idée du Ligthning Network est de proposer une surcouche au réseau Bitcoin pour passer certaines transactions off chain sur un canal de paiement. Les seules transactions enregistrées sur la Blockchain seront l'ouverture et la fermeture du canal de paiement. Le Lightning Network permet d'accélérer considérablement la vitesse des transactions, et d'alléger également sensiblement les frais.

Liquidation
On parle de liquidation lorsqu'une position est liquidée avec le déficit maximum autorisé par le broker pour la position prise. La liquidation n'est pas souhaitable et résulte en principe d'une mauvaise stratégie de trading. Il est donc important de soigner sa gestion du risque et de prévoir différents scénarios pour éviter à tout prix ce type de situation.

MVP

Le terme “MVP” est l’acronyme de “minimum viable product”. Celui-ci est généralement cité dans le phénomène des startups, que l’on retrouve avec les projets se finançant par une ICO. Le MVP désigne alors le produit, ou la stratégie permettant d’offrir l’innovation promise de la manière la plus simple et rapide possible. Cela permet de démontrer aux investisseurs la capacité d’exécution de la startup, qui bénéficie également des retours de sa communauté lui permettant de faire évoluer son produit en fonction de ses utilisateurs, sans partir dans des développements longs et couteux qui l’éloigneraient de son marché.

MACD

L’acronyme MACD signifie Moving Average Convergence Divergence. Il s’agit d’un indicateur technique permettant de déterminer les changements de tendance. Le MACD est la différence entre deux moyennes mobiles exponentielles de périodes différentes (généralement de 12 et 26 jours). Les MACD sont utiles lorsqu’on les croise avec sa ligne de signal, pour déterminer un signal d’achat ou de vente.

Maker

Le « maker » est un ordre d’achat ou de vente dans l’order book d’un broker ou d’une plateforme de trading. À la base, les market makers sont des intermédiaires comme les brokers, qui cotent des marchés pour investisseurs et dégagent une marge (un spread) entre les prix d’achat et de vente pour se rémunérer. Le prix d’achat proposé est donc légèrement supérieur à celui du marché, et le prix de vente légèrement inférieur. Par extension, on appelle un « maker » une personne qui passe un ordre d’achat ou de vente sur l’order book à un prix différent de celui du cours actuel. Son ordre sera donc exécuté en différé.

Market

Un marché dans les cryptomonnaies désigne une paire sur un exchange, par exemple ETH/EUR sur Kraken, c’est-à-dire tous les échanges entre ethers et euros sur cet exchange. Un exchange propose donc autant de marchés que de paires qui peuvent être une cryptomonnaie et une monnaie fiat (par exemple BTC/JPY) ou deux cryptomonnaies (par exemple ZEC/BTC).

Mineur

Un mineur est une personne ou une entreprise qui investit dans un ou des ordinateurs et dépense de fortes sommes en électricité pour miner des cryptomonnaies. Le rôle d’un mineur dans le système PoW est donc de contribuer par son travail à déterminer le consensus dans une blockchain, en respectant le protocole de création des blocs à la lettre, en étant le premier à satisfaire le niveau de difficulté du moment et en soumettant un bloc validé par la majorité des nœuds du réseau.

Mt Gox

Mt Gox est une plateforme d'échange créée en 2009 proposant à l'origine l'échange de cartes Magic:The Gathering Online. En 2010, elle est reconvertie en plateforme d'échange de bitcoins et sera rachetée par Mark Karpelès en 2011, qui la propulsera pour en faire la plateforme incontournable du marché. En 2014, Mt Gox brasse 80% du volume d'échange de bitcoins, avant de fermer brutalement suite au constat d'un trou de 650 000 bitcoins dans les caisses de la plateforme. Les procédures de remboursement des victimes sont toujours en cours en 2018.

Mainnet
Le mainnet est le réseau original permettant de transférer une cryptomonnaie d'une adresse à l'autre au sein de la blockchain. Le mainnet se distingue du testnet, qui a pour vocation de tester la fonction de transfert sur un réseau prototype. De très nombreuses cryptomonnaies n'en sont qu'à cette étape et ne disposent donc pas encore d'un mainnet. Les tokens d'un projet sans mainnet ne peuvent avoir d'autre utilité que celle du trading, ou à défaut de matérialiser la somme investie par des tokens provisoires. À la sortie du mainnet, on aura recours à ce que l'on appelle un « token swap » pour obtenir les tokens définitifs.

Minting
Le minting se distingue du mining, qui désigne en anglais le fait de miner une cryptomonnaie reposant sur un consensus de preuve de travail. Le minting désigne donc quant à lui le fait de forger les blocs d'une cryptomonnaie reposant sur une blockchain de preuve d'enjeu. En français, on parlera vulgairement de « forgeage » pour faire référence au minting, de sorte à le distinguer clairement du minage.

Mineable
L'adjectif "mineable", que l'on retrouve notamment chez Coin Market Cap, désigne les coins dont l'algorithme de consensus est le Proof of work (preuve de travail, voir entrée correspondante). On peut donc les miner et investir dans du matériel informatique de pointe pour essayer d'être le premier à trouver la bonne empreinte pour ajouter son bloc à la chaîne et toucher la récompense correspondante. L'ether devrait cesser d'être mineable prochainement pour passer au Proof of Stake.

Malta AI & Blockchain Summit
Le MAIBS est le plus grand congrès ("business") sur les cryptomonnaies en Europe. Il se tient deux fois par an en Mai et en Novembre et rassemble de nombreux acteurs des secteurs de la blockchain et de l'IA sur l'île de Malte. Conférences, Workshop, Expositions et Networking sont bien sûr de la partie lors de l'évènement.

Margin trading
Le margin trading consiste à emprunter de l'argent pour bénéficier d'un effet de levier dans le cadre de ses activités de trading. Le margin trading permet d'amplifier ses

gains, mais a également pour effet de décupler les pertes. Il s'agit donc d'une pratique pouvant être très risquée. Certaines plateformes comme BitMEX sont spécialisées en margin trading et proposent plusieurs cryptomonnaies pour donner plus de choix aux traders.

Mark Karpelès
Mark Marpelès est l'ancien dirigeant de la plateforme d'échange MtGox, la plus grosse plateforme d'échange de bitcoins en 2014. Arrêté en 2014 suite à la volatilisation de 650 000 bitcoins manquants dans les comptes de Mt Gox, Mark Karpelès a toujours clamé son innocence. Il reste au sein de la communauté crypto un des personnages les plus détestés et est encore aujourd'hui considéré comme coupable par la majorité des investisseurs lésés. Mark Karpelès est d'autant plus suspect que ce dernier avait déjà été reconnu coupable pour détournement de données auprès d'un de ses précédents employeurs.

Market Cap
Market Cap est une expression anglaise qui signifie capitalisation du marché. C'est la valeur, généralement exprimée par défaut en USD, que représente une cryptomonnaie donnée. On calcule le market cap en multipliant le nombre de jetons en circulation par le cours de la monnaie. Le site Coin Market Cap le calcule en fonction du cours moyen pondéré des exchanges où sont cotées les cryptomonnaies.

Masternode
Un masternode est récompensé en coins à chaque fois que celui-ci ajoute et valide un bloc. L'ajout de chaque bloc et donc les récompenses correspondantes sont attribuées aléatoirement aux différents masternodes. En plus des récompenses, un protocole PoS peut proposer d'utiliser des sanctions économiques pour prévenir les attaques d'hackers. Si une attaque est détectée, le protocole peut prévoir d'appliquer un système de pénalité au forgeur pirate, qui perdrait automatiquement ses coins mis en dépôt.

Minage/Mining
Le minage, ou mining en anglais, désigne le processus permettant de résoudre un problème mathématique ou un défi informatique imposé par le consensus de preuve de travail (Proof-of-Work en anglais, ou PoW) d'une blockchain. L'activité de minage exige une puissance de calcul variable en fonction de l'algorithme de la blockchain et de la difficulté de minage. Cette activité permet de valider et traiter les transactions tout en maintenant la sécurité et la synchronisation du réseau. Les mineurs sont récompensés pour leur travail par la génération et/ou la distribution de nouveaux jetons.

Nonce

En cryptographie, un nonce est un nombre aléatoire, destiné à être utilisé une seule fois, qui est ajouté à une suite de caractères immuable pour trouver une nouvelle empreinte (hash) lors du passage par un logiciel de chiffrement. Comme la longue suite de caractères formée par un bloc est bien immuable, les mineurs n'ont d'autre choix que d'essayer des milliards de nonces pour chaque bloc, jusqu'à trouver celui qui permette d'aboutir à un hash satisfaisant le niveau de difficulté du moment pour que son bloc soit accepté par le réseau.

Nick Szabo

Nick Szabo est à la fois juriste, informaticien et cryptographe, et ses travaux sont à l'origine de la création des cryptomonnaies et des smart contracts. L'expression et le concept de smart contract est pour la première fois développé par Nick Szabo afin d'améliorer le droit des contrats et faciliter les protocoles d'e-commerce entre étrangers. Celui-ci est également à l'origine d'un mécanisme de cryptomonnaie appelé Bit Gold conçu en 1998. Bien que n'ayant pas remporté le soutien de la population, Bit Gold pose les bases de l'architecture Bitcoin.

Nœuds/nodes

Les nœuds sont les participants à un réseau pair à pair qui assurent certaines fonctions non rémunérées de sauvegarde, validation, vérification ou transfert de données, s'ils ne se livrent pas à du minage (PoW) ou du minting (PoS). Dans le réseau d'une blockchain comme celle de Bitcoin par exemple, un nœud est un ordinateur qui stocke l'intégralité du registre (toutes les transactions ayant eu lieu depuis la création de la cryptomonnaie) et qui transfère les requêtes des utilisateurs aux mineurs. Le nombre et la disponibilité des nœuds sont des facteurs importants de qualité et fiabilité d'un réseau décentralisé.

Oracle

Les oracles sont des pourvoyeurs d'informations professionnels, neutres et certifiés. Un oracle est souvent une personne mais peut également être une application qui récolte directement ou indirectement dans le monde réel un type bien précis d'informations, les entrent dans les réseaux de blockchains et est rémunérée par les détenteurs ou ayant-droits des blockchains. Les oracles interviennent quand une injection de données provenant de sources très précises extérieures au réseau (services météo par exemple) ou de constatations que seules des personnes peuvent effectuer est nécessaire. Les oracles sont des acteurs indispensables de certains contrats intelligents gérés par blockchain et des marchés prédictifs.

Order book

L'order book signifie « carnet d'ordres » en français. Il s'agit de la liste des ordres d'achat ou vente d'un marché, que l'on peut observer pour chaque cryptomonnaie sur une plateforme d'échange. L'order book est mis à jour en temps réel tout au long de la

journée et peut donner des informations sur les anticipations des autres traders des mouvements de marché.

Over The Counter/Gré à Gré

Over the counter, abrégé OTC, ou de “gré à gré” en français, est un type de transaction financière dans laquelle deux personnes physiques ou entités sont mises directement en relation pour échanger des actifs, donc sans passer par une plateforme boursière ou un exchange, généralement avec de fortes sommes d’argent en jeu.Dans le monde des cryptomonnaies, les exchanges les plus importants proposent cette fonctionnalité à partir d’un certain montant assez élevé. Ce type de transaction occasionne donc des frais plus élevés que le fait de simplement utiliser l’exchange pour vendre ou acheter, mais présente l’avantage de la discrétion, car le prix de la transaction n’est pas divulgué, et une certaine forme de sécurité car les deux personnes ou entités sont mises directement en relation et peuvent se rencontrer physiquement pour effectuer la transaction. Les transactions de gré à gré permettent par ailleurs d’échanger des actifs dont la qualité ou la quantité se prêtent mal aux normes des plateformes boursières.Enfin, une transaction OTC permet aux deux parties de s’assurer contre le défaut de paiement de l’autre partie comme sur une plateforme boursière ou un exchange, mais en utilisant d’autres mécanismes. Il faut savoir qu’aux États-Unis, environ 40% des transactions d’actions se font de gré à gré.

PIP

Le pip est une unité de mesure que l’on utilise sur le marché du Forex, mais qui peut également s’utiliser en cryptomonnaie, notamment pour les CFD. Un pip définit le changement de valeur entre deux devises et représente le plus petit mouvement qu’une devise peut faire. En trading ou en investissement, on utilise le pip pour calculer le spread (l’écart) entre le cours d’achat et le cours de vente d’une paire de devises, placer un Stop Loss ou un Take Profit.

PIHR

Une PIHR, plateforme d’investissement à haut rendement, HYIP ou high yield investment platform en anglais, est un type d’investissement frauduleux de type pyramide de Ponzi qui a connu une nouvelle jeunesse avec les cryptomonnaies et a fait beaucoup de vicitimes fin 2017 avec l’envolée du cours des cryptomonnaies, la plus emblématique d’entre elles ayant été Bitconnect.

Pump

Un pump est une hausse brutale et soutenue du cours d’un actif. Le contraire du pump est le dump. Un pump reste un mouvement assez violent sur un marché, et génère souvent d’autres mécanismes par effet boule de neige.

Plasma

Le projet Plasma est mené conjointement par Joseph Poon et Vitalik Buterin et vise à améliorer la scalabilité et la rapidité d'Ethereum. Le projet Plasma est assimilable à ce qu'apporte le Lightning Network à Bitcoin et consiste à proposer une surcouche à la blockchain Ethereum afin d'alléger le réseau. Le projet prévoit que toutes les données des transactions soient agrégées sur la blockchain Plasma, qui communiquera avec la blockchain Ethereum pour valider les blocs en toute sécurité. Le but de Plasma est de permettre à Ethereum de supporter plusieurs milliers voire centaines de milliers de transactions par secondes (contre 20 transactions par secondes aujourd'hui).

Poloniex
Comme Bittrex et Binance, Poloniex est un exchange majeur spécialisé dans les altcoins et n'acceptant pas les monnaies fiat.

Panic sell
Le « panic sell » (vente panique) consiste à vendre une cryptomonnaie dans l'urgence par peur que le cours ne s'effondre. Cela se produit souvent sur le marché des cryptomonnaies dès qu'une mauvaise nouvelle est annoncée, ou que la chute d'un cours s'accélère brutalement. Les traders les plus expérimentés et les mieux formés ne cèdent pas au panic sell et parviennent à maintenir une bonne gestion du risque pour éviter les décisions précipitées et non réfléchies.

Paper wallet
Un paper wallet est un portefeuille physique permettant d'imprimer sa clé privée sur papier afin de la conserver en lieu sûr (le mieux étant un coffre fort) et de ne s'en servir qu'au moment voulu. Le paper wallet est un cold storage, ou « stockage à froid », qui est idéal pour sécuriser ses avoirs sur le long terme (plusieurs mois, voire plusieurs années). Il est en revanche très peu pratique si vous souhaitez régulièrement vous connecter à votre wallet pour envoyer des fonds. Le paper wallet n'est par exemple pas adapté si vous souhaitez mener des activités de trading avec les fonds qu'il contient.

Peer to peer
Un réseau peer to peer, de pair à pair en français, est un réseau sans organe ou serveur central, où chaque ordinateur peut jouer le rôle de client ou de serveur, c'est-à-dire qu'il peut proposer tous les services d'un serveur central, à savoir le stockage et le traitement de données, l'attribution de tâches, la communication d'informations et de données, et être lui même client du réseau, c'est-à-dire émettre des requêtes.Un système peer to peer n'est pas forcément décentralisé, mais il l'est pour presque toutes les cryptomonnaies. Il permet, par exemple, de mettre en place un partage de fichiers comme dans le cas de Bittorrent, ou un calcul distribué comme dans le cas des cryptomonnaies. Il donne aussi un avantage conséquent en terme de sécurité, car les fonctions et données primordiales du réseau ne sont pas concentrées sur un

serveur central, mais réparties sur tous les nœuds du réseau, si bien que seule l'interruption d'Internet pourrait rendre le réseau inopérant.

Point d'entrée
Lorsque l'on fait référence au point d'entrée sans plus de précision, on fait en réalité référence au point d'entrée dans une prise de position de trading. La prise de position peut être longue ou courte, mais dans tous les cas, son point d'entrée sera déterminant sur la réussite du trade. Un mauvais point d'entrée peut rendre la sortie très difficile. Savoir fixer son point d'entrée est donc déterminant pour mener une stratégie de trading efficace et viable sur le long terme.

Point de sortie
Le point de sortie désigne le moment où un trader clôt sa position. La sortie peut donc se solder sur un gain une perte en fonction du point d'entrée. Le point de sortie est plus difficile à déterminer que le point d'entrée pour beaucoup de traders. Cela est encore plus vrai sur le marché des cryptomonnaies, qui est très difficilement prévisible. Définir son point de sortie exige donc d'avoir un plan de trading et de gestion du risque, et de toujours croiser son analyse fondamentale avec son analyse technique sans laisser ses émotions prendre le dessus.

Practical Byzantine Fault Tolerance
L'objectif des protocoles Byzantine Fault Tolerance (BFT) est de permettre à un réseau distribué d'atteindre un consensus suffisant malgré la présence de noeuds malicieux ou défectueux dans le système. Ces noeuds pourraient en effet communiquer des informations incorrectes au reste du réseau et mettre en péril sa pérennité. Le but d'un BFT est de protéger le réseau contre ces failles byzantines (« Byzantine Failures ») en réduisant leur influence.L'algorithme Practical Byzantine Fault Tolerance (pBFT), introduit en 1999 par Miguel Castro et Barbara Liskov, fait partie des différents protocoles BFT et est aujourd'hui l'un des plus populaires. Celui-ci a l'avantage de pouvoir effectuer des dizaines de milliers de transactions par secondes et maintient la sécurité du réseau tant que moins d'un tiers de ses noeuds sont malicieux. L'algorithme pBFT est tout à fait adapté aux blockchains privées et est notamment utilisé par Hyperledger.

Proof of Stake
Le Proof of stake, preuve d'enjeu en français, est un des mécanismes de consensus blockchain les plus répandus. L'idée de cet algorithme est d'attribuer la détermination du consensus par l'ajout de blocs à la blockchain à des nœuds appelés masternodes qui détiennent un certain montant des coins de la blockchain en question. Ce montant est systématiquement clairement indiqué par l'émetteur de la cryptomonnaie.

Proof of Work

La Proof of work, preuve de travail en français, est un des deux grands algorithmes de consensus pour blockchain. C'est aussi le plus ancien, puisque Bitcoin se base sur ce protocole de consensus. Dans une blockchain publique, un algorithme de consensus sert à désigner le bloc qui est ajouté à la blockchain à un instant T et donc la "vérité" de cette blockchain. Créer des blocs de transactions est facile pour un ordinateur connecté au réseau. Il faut donc un procédé permettant de déterminer pour chaque bloc un seul et unique participant l'ajoutera à la chaîne, car celle-ci doit être unique.L'idée de la Proof of work est d'exiger des mineurs d'effectuer un certain travail, à savoir résoudre un problème mathématique très difficile dont la solution ne pourra être trouvée que par hasard, pour leur permettre d'ajouter leur bloc à la chaîne et ainsi de déterminer le consensus à un instant T. Ils pourront alors toucher une rémunération (12,5 bitcoins par bloc pour le cas actuel de Bitcoin).Le problème majeur du Proof of work est qu'il engendre une dépense énergétique phénoménale car les mineurs se livrent à une course à la puissance pour être capables de résoudre les premiers ce problème mathématique et empocher ainsi les récompenses. Il favorise par ailleurs les mineurs ayant le plus de moyens pour investir dans du matériel informatique et de l'électricité.

Psychologie des foules

La psychologie des foules fait référence aux comportements de masse que l'on peut observer dans telle ou telle situation. En trading, il est essentiel de cerner la psychologie des foules et de l'anticiper pour construire une stratégie gagnante. Le comportement et les actions de la foule en tant qu'entité sont fortement influencés par la perte de responsabilité des individus. Le rôle du trader est de conserver sa responsabilité et de se positionner en tant que spectateur de la foule pour adapter ses positions en fonction de ses comportements.

Public address/Private key

Le couple public/private key est fondamental en cryptographie asymétrique et se matérialise chez les cryptomonnaies sous la forme de public address/private key (adresse publique/clé privée en français). La public address est comme un IBAN: elle sert à recevoir des coins et est propre à une cryptomonnaie donnée. On peut la diffuser au monde entier car il est théoriquement impossible de déterminer sa private key. La private key nous donne le contrôle d'une public address et donc des fonds qui y sont rattachés. Il est très facile de générer des public addresses à partir de private keys, mais l'inverse est impossible: c'est le principe de la cryptographie asymétrique.

ROI

ROI est acronyme anglais pour Return on Investment, « retour sur investissement » en français. Le ROI donne une indication très importante sur la rentabilité d'un investissement un d'un trade. Il est calculé en faisant le rapport du profit obtenu sur le montant investi. Un titre d'exemple, un ROI de 100% signifie faire un "fois deux" – doubler sa mise de départ.

Root
Sur chaque système informatique, il existe plusieurs niveaux de droits. Sur Windows par exemple, la session invitée permet de limiter fortement le nombre de permissions sur l'ordinateur.

Avoir un périphérique "rooted" signifie tout simplement que l'on a accès au niveau de droit le plus important possible. Cela a des avantages et des inconvénients. L'avantage principal est que vous pourrez modifier absolument tous les paramètres, mais si jamais un individu entrait en possession de votre périphérique, il pourrait également avoir facilement accès aux paramètres les plus sensibles.

Andrea Antonopoulos prévient dans une de ses vidéos que les téléphones mobiles sont généralement plus sécurisés que les ordinateurs et qu'il est donc préférable d'y stocker vos bitcoins. Cependant, de plus en plus de téléphones sont "root" par les utilisateurs pour débloquer des fonctions. C'est le fameux jailbreak de l'iPhone. Dans ce cas là, stocker vos bitcoins sur votre téléphone n'est pas recommandé, et d'une manière générale il faudra vous tourner vers un hardware wallet.

Range
En finance, le range est, comme sa traduction en français l'indique, une fourchette de prix dans lequel un investisseur pense qu'un actif va évoluer durant une certaine période.

Raiden Network
Le Raiden Network propose une solution de « scaling off-chain » pour Ethereum afin d'aider la blockchain à pouvoir suivre une fréquence de transactions plus élevée sans avoir à faire de fork. Le réseau fonctionne avec un système de state channels, autrement dit des zones permettant de gérer des transactions hors blockchain. Les states channels permettent aussi bien d'accélérer la vitesse de transaction que d'en diminuer les coûts. Tout comme le projet Plasma, Raiden vise donc à améliorer la performance du réseau Ethereum.

Résistance
Les niveaux de support et résistance sont des fondamentaux de l'analyse technique en trading. Une résistance est un seuil à partir duquel les mouvements baissiers freinent la hausse des cours : on observe donc un certain palier, que le cours d'une cryptomonnaie ne semble jamais ou alors très rarement dépasser. Ce seuil peut être considéré comme un signal de vente intéressant. Très souvent, une fois atteint, il entraîne donc une correction baissière. Mais la difficulté reste de savoir identifier correctement un niveau de résistance.

Retracements de Fibonacci

Les retracements de Fibonnacci sont une méthode utilisée pour fixer des objectifs de cours pendant une phase de consolidation. L'idée est d'évaluer le niveau des corrections ou des rebonds pour se positionner correctement sur une tendance.Dans cette suite, chaque nombre est égal à l'addition des deux chiffres précédents: 1,1,2,3,5,8,13,21...Cette suite nous a permis de découvrir le nombre d'or 1,618 et le ratio d'or 0,618. Chaque nombre de la suite est plus ou moins égal à 0,618 fois le nombre suivant et 1,618 fois le nombre précédent. C'est à partir du ratio d'or que l'on peut déterminer les retracements de Fibonacci.

Scam

Scam est un terme argotique anglais signifiant « arnaque », il s'agit d'une escroquerie tout simplement. Un projet est un « scam » lorsque les instigateurs de celui-ci partent avec les fonds des investisseurs, par exemple.

Spot

Le prix « spot » est le prix comptant d'un actif. Ce prix est fixé pour une livraison immédiate sur un marché au comptant, par opposition au marché des futures. Le marché spot assure à l'investisseur la stabilité du prix et est donc moins risqué que le marché des futures.

Segwit

Segwit est une mise à jour (soft fork) appliquée en août 2017 à la blockchain de Bitcoin, et ensuite à celles d'autres monnaies telles que Litecoin, Digibyte ou Vertcoin qui signifie "segregated witness", "témoin ségrégué" en traduction littérale. Le but de Segwit est d'augmenter la scalabilité du réseau en diminuant la taille des transactions id (Tx-ID). Ce système contourne le fait que la taille des blocs ne peut pas être augmentée en changeant la manière de comptabiliser l'espace d'octets à unités, ce tour de passe passe faisant gonfler la taille maximum d'un bloc de 1 à 1,8 Mo.Les données de chaque transaction sont séparées en deux parties: les informations sur le donneur, le receveur et la transaction d'une part (public addresses et nombre de coins transmis), qui ne sont pas modifiées par Segwit, et la nouvelle structure « witness » (témoin) qui contient les scripts et signatures de validation, et prend quatre fois moins de place que dans le système pré-Segwit. Les signatures sont séparées de leur transaction et mises bout à bout ensemble à la fin des séries de chiffres et de lettres constituées par les mineurs pour former des blocs. En sortant la signature de la Tx-ID, Segwit rend par ailleurs cette dernière impossible à modifier.

Spread

Le spread est l'écart entre le prix d'offre d'achat (Ask) et de vente (Bid) d'un actif. Il peut aussi désigner l'écart de prix entre deux plateformes d'échange et permettre de réaliser un arbitrage.

Satcoin
Un satcoin est un coin qui vaut quelques satoshis, soit pratiquement rien.

Satoshi
Un satoshi, du nom du mystérieux inventeur du bitcoin, est une unité de compte qui représente un cent millionième de bitcoin, soit très peu d'argent. C'est la fraction la plus petite d'un bitcoin.

Support
Un support est un seuil à partir duquel on les mouvements haussiers freinent la baisse des prix. Il est donc le contraire d'une résistance. Le support peut donc correspondre à une fin de période baissière et annoncer la reprise à la hausse d'un cours. Un support est donc un point d'entrée intéressant pour les acheteurs. Sur le marché des cryptomonnaies, les supports sont plus difficiles à déterminer que sur des marchés stables, car les valeurs sont beaucoup plus volatiles et cassent fréquemment leurs niveaux de supports et résistances.

Scalping
Le scalping est un mode de trading très rapide assimilable au microtrading. Les prises de position ne durent que quelques secondes à quelques minutes. Très souvent, le scalping se fait sur futures ou sur CFD. Le scalping est particulièrement efficace sur des périodes de range avec très peu de volatilité. On distingue le scalping du day trading ou du swing trading, pour lesquels les positions sont beaucoup plus longues.

Sharding
Le sharding est le fait de partitionner une blockchain en vue d'améliorer sa scalabilité. Un sharding est prévu pour la blockchain Ethereum. L'objectif est d'augmenter le nombre de transactions par seconde sur le réseau, en partitionnant toutes les ressources de calcul en fragments afin que chaque nœud n'ait plus à traiter que des fragments de l'état de la blockchain pour opérer plus vite. Le sharding vise à passer de 15 transactions par secondes à 1 million de transactions par secondes. A noter que la scalabilité d'Ethereum fait l'objet de plusieurs autres projets, comme Plasma et le Raiden Network.

Shitcoin
Un shitcoin est une cryptomonnaie n'ayant aucun projet viable, aucune base technique sérieuse et donc aucune valeur intrinsèque. Ce type de coin est souvent utilisé pour spéculer afin de profiter de la volatilité d'un cours. Certains projets de shitcoins sont cependant des arnaques très bien déguisées pouvant facilement tromper des investisseurs un peu trop dupes. Il est donc très important de se renseigner précisément sur chaque projet avant se procurer des tokens.

Soft cap
Un soft cap est un terme propre aux ICO. Ce terme désigne le montant minimum qu'une entité doit lever pour pouvoir mener son projet. En théorie, lorsque le soft cap n'est pas atteint, le projet a peu de chances d'aboutir et considère qu'il ne pourra pas mener à bien ses activités de développement faute d'un budget suffisant. Souvent, l'ICO est donc annulée et les fonds reversés aux participants. Les fondateurs peuvent cependant décider de poursuivre leur projet, même lorsque le soft cap n'est pas atteint.

Solidity
Solidity est le langage de programmation initialement utilisé par Ethereum pour le développement des smart contracts et des DApps. De nombreuses blockchains l'ont repris mais Ethereum reste aujourd'hui un leader incontesté dans son domaine. D'autres blockchains proposent des alternatives permettant aux développeurs d'éviter d'avoir à apprendre le Solidity, qui reste assez complexe. C'est par exemple le cas de Lisk, qui offre la possibilité de développer des DApps en JavaScript.

Sidechain
Une sidechain est une blockchain fille rattachée à une blockchain mère. Le but de cette architecture est de pouvoir segmenter les informations afin d'augmenter le volume d'informations traitées tout en rendant possible la communication entre la chaîne mère et les chaînes filles. L'architecture en sidechain est une réponse aux problèmes de scalabilité que rencontrent les blockchains de première et seconde génération, qui doivent aujourd'hui trouver des solutions pour augmenter leur nombre de transactions par seconde. Des projets comme Ardor ou Lisk sont basés sur des sidechains et suscitent un vif intérêt auprès de la communauté crypto.

Stop Loss
Le stop loss est un type d'ordre en finance qui consiste à indiquer à la place de marché que l'on est prêt à acheter ou vendre un actif lorsqu'il a atteint un certain prix. Si ce prix (stop price en anglais, ou seuil de déclenchement en français) est atteint, l'ordre stop loss devient un ordre d'achat ou de vente normal et sera exécuté plus ou moins rapidement en fonction de la liquidité du marché.

Scalabilité
Le mot « scalabilité » est un néologisme reprenant le verbe anglais « to scale », qui signifie « mettre à l'échelle ». La scalabilité désigne la capacité d'un système à pouvoir opérer avec la même efficacité à une échelle supérieure, par exemple avec des centaines de millions d'utilisateurs supplémentaires par rapport à un instant T. La scalabilité est un problème majeur des blockchains et fait l'objet de nombreuses réflexions, aussi bien pour Bitcoin que pour Ethereum. Les blockchains de nouvelle génération en font une priorité pour pouvoir prétendre à une adoption massive.

Security token
Un security token attribue à son investisseur un droit de récompense qui lui permet d'être rémunéré en fonction de la richesse créée par l'entreprise. Le security se distingue de l'equity token, qui attribue un droit de possession d'un titre et correspond donc à une participation au capital de l'entreprise. On peut en quelque sorte rapprocher les security tokens des ETFs ou des fonds mutuels. Globalement, ce type d'actifs reste cependant très propre à la blockchain.

Short Selling
En finance, le short selling, ou vente à découvert en français, consiste à vendre un actif qu'on ne détient pas le jour de la vente mais que l'on se procurera le jour où celui-ci doit être livré. La personne qui vend à découvert parie donc sur la baisse du prix de l'actif, qui peut être une action, une devise, une matière première ou une cryptomonnaie, car elle espère acheter le jour de la livraison l'actif moins cher que le jour où elle l'a vendu (à découvert), ce qui suppose que son prix aurait baissé. On dit dans ce cas que le vendeur à découvert a une position courte et le détenteur d'un titre une position longue.

Signature numérique
La signature numérique, ou électronique, est un procédé permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur. La plupart recourent à la cryptographie asymétrique, notamment dans le cas des cryptomonnaies. Un tel procédé doit permettre d'identifier la personne ou l'organisme qui a apposé sa signature, et de garantir que le document n'a pas été altéré entre le moment où la personne ou l'organisme appose sa signature et celui où le lecteur le consulte.Ce procédé est constamment utilisé dans les systèmes de cryptomonnaies pour valider les transactions: la signature numérique, qui varie suivant chaque monnaie, permet à l'émetteur d'une requête de montrer qu'il est bien le détenteur de la clef privée associée à l'adresse publique qu'il utilise, sans avoir à dévoiler cette clef privée, ce qui enlèverait tout intérêt au système. La signature numérique permet également de garantir le fait que la transaction n'a pas été modifiée lors de son court passage sur le réseau : le moindre changement des données de la transaction modifierait complètement la signature électronique.

Stablecoin
Un stablecoin est un coin qui réplique la valeur d'un actif stable généralement en dehors du monde des cryptomonnaies, le dollar US ou l'or par exemple, faisant d'eux des valeurs refuges pour les investisseurs qui veulent se protéger contre la forte volatilité du marché des cryptomonnaies sans en sortir. En effet, lorsqu'un investisseur pense que le marché des cryptomonnaies va baisser, il achète des stablecoins (Tether notamment), et les vend contre des cryptomonnaies lorsqu'il pense que le marché va monter, si bien que les paires BTC/USDT (Bitcoin/Tether) et ETH/USDT sont systématiquement les premières paires d'échanges de ces monnaies.

Stop Limit
Stop Limit est un ordre permettant d'acheter ou de vendre une cryptomonnaie à la condition que son cours se situe dans la fourchette de 2 montants : le "stop" et le "limit".Le principe est d'avoir une meilleure maîtrise de ses ordres qu'avec un simple stop loss, car il arrive de voir l'ordre dépasser largement le seuil envisagé. Le stop limit permet donc de définir une fourchette en dehors de laquelle une vente ou un achat ne pourra avoir lieu.

Swing Trading
Le swing trading désigne des opérations de trading avec des prises de positions plutôt longues. L'écart de temps entre l'ouverture et la fermeture des ordres dépasse les 24h, le swing trading implique donc une prise de position plus longue qu'en day trading. Le but consiste à entrer sur le marché au début d'une tendance et à en sortir au moment où celle-ci s'essouffle. La difficulté est donc de trouver un bon point d'entrée, mais surtout un bon point de sortie, pour maximiser ses gains tout en minimisant ses pertes.

Taker
Un taker est un trader ou un investisseur qui achète au prix du marché. Son ordre d'achat ou de vente sera donc exécuté immédiatement. Le taker lit l'order book et achète ou vend au prix le plus satisfaisant du moment. Les takers achètent et vendent au prix du marché, tandis que les makers agissent sur les prix du marché en définissant des prix de vente ou d'achat à la hausse ou à la baisse.

Token
On distingue le token du coin, bien qu'il n'y ait pas encore de consensus clair sur leur définition et des différence entre un token et un coin. Un token peut être considéré comme un bon d'achat numérique dont l'unicité est prouvable mathématiquement et pouvant être échangé contre des actifs, services ou biens. Ether est aussi bien un coin qu'un token: c'est un coin dans son rôle de monnaie comme unité de compte, réserve de valeur ou intermédiaire des échanges. C'est aussi un token dans sa capacité à donner accès à un service, lorsque l'on s'en sert pour payer du Gas et ainsi avoir accès aux fonctionnalités de l'EVM. Par conséquent, les pure "coins" (Bitcoin, Monero, Dash, Litecoin etc.) ne peuvent être que des coins. Mais REM, DFT, LSK, EOS, GNT, STRAT et bien d'autres peuvent être aussi bien des coins que des tokens.La définition de CoinMarketCap est différente et considère qu'un token est une cryptomonnaie qui n'a pas (encore) sa propre blockchain. Un token est créé généralement sur la blockchain de l'ETH, mais cela peut être aussi sur celle de Next, Omni, Counterparty ou encore Neo. Selon cette définition, un coin est une cryptomonnaie ayant sa propre blockchain.Le concept de token ne provient pas directement de l'écosystème des cryptomonnaies: il est bien plus ancien. Un token désignait il y a déjà plusieurs siècles, en Angleterre notamment, une monnaie parallèle à l'unité monétaire nationale émise par une guilde, un groupe de commerçants, ou encore une ville, et acceptée par le pouvoir en place.

Tangle
Le Tangle est une architecture de DLT basée sur un DAG (Directed Acyclic Graph / graphe orienté acyclique). IOTA est à l'origine du terme et est la première à proposer sa mise en application. Dans le Tangle, une transaction valide deux transactions passées. Le consensus n'est pas géré par une partie du réseau (mineurs ou forgeurs), mais par l'ensemble des participants actifs (soit des appareils réalisant des transactions). Le Tangle est donc hautement décentralisé, mais faiblement sécurisé.

Tether
Le tether est un stablecoin arrimé à la valeur du dollar US. La seule fonction du tether est donc de toujours valoir un dollar US. Son rôle est très important pour le marché des cryptomonnaies, car il permet aux investisseurs de rester dans ce marché même quand il baisse au lieu de revendre leurs cryptomonnaies pour des monnaies fiat.Le tether est toujours dans les vingt premières capitalisations boursières: c'est donc un poids lourd du marché en tant que valeur refuge. Pour que la valeur du tether soit toujours stable et reste à 1 tether = 1 dollar, Tether Ltd émet et vend des tokens pour agir en permanence sur le cours comme un régulateur.Le tether est largement utilisé pour acheter des cryptomonnaies, notamment du bitcoin et et de l'ether. Autour de 30% des ETH sont achetés en effet en USDT. Si le tether venait à s'effondrer car on s'apercevrait que Tether Ltd ne détient pas les 2,5 milliards de dollars correspondant au nombre de tethers en circulation, il pourrait emporter tout le marché avec lui en l'espace de quelques jours. D'autres stablecoins sont cependant en train de voir le jour et tether ne sera bientôt plus la seule valeur refuge du marché des cryptomonnaies.

Ticker
Toutes les monnaies fiat et les cryptomonnaies sont représentées sur les marchés par un symbole appelé ticker, comme BCH pour le bitcoin cash, USD pour le dollar US ou DFT pour Draftcoin.

Trader
Un trader, ou opérateur de marché en français, est un négociateur de produits financiers qui peuvent être des actions, des obligations, des cryptomonnaies, des produits dérivés, et qui intervient sur les marchés organisés ou de gré à gré. Un trader travaille habituellement dans une salle des marchés aux horaires de la place de marché sur laquelle il intervient, mais cela est amené à changer avec le fait que les marchés de cryptomonnaies fonctionnent 24h/24 et 7j/7. Un particulier peut également proposer ses services de trading s'il a acquis une expertise dans ce domaine en étant par exemple spécialisé sur une certaine place de marché ou un certain type de produits financiers.

Testnet

Un testnet (réseau de test) est un prototype de mainnet utilisé pour effectuer des tests sur le protocole et le réseau sans risquer de léser les utilisateurs. Le lancement d'un testnet est une première bonne nouvelle pour une blockchain, car il permet d'avoir un prototype à montrer aux investisseurs pour témoigner des avancées du projet. C'est cependant lorsqu'une blockchain lance son mainnet qu'elle est pleinement opérationnelle et que ses tokens ont une véritable valeur. Avant cette étape, tout investissement reste un gros pari sur l'avenir, et un projet de blockchain peut tout à fait de jamais lancer son mainnet.

Trading
Le trading est l'activité exercée par un trader, à savoir le négoce (achat et vente) de produits financiers dans le but de dégager un profit.

Take profit
Take profit est une opération boursière consistant à quitter un marché en vendant car on considère que l'actif coté a pris suffisamment de valeur et que son cours devrait baisser très prochainement. Cela ne signifie pas que l'investisseur ne reviendra pas sur ce marché: il le fera probablement lorsque le cours de l'actif aura suffisamment baissé ou s'il repart au contraire fortement à la hausse.

To the moon
« To the moon » est une expression très fréquemment utilisée par les communautés cryptos. Elle désigne l'enthousiasme pour une cryptomonnaie, dont ses investisseurs voient croître la valeur « to the moon » (jusqu'à la Lune). L'expression revient souvent en période haussière ou quand une monnaie fait un pump. On retrouve généralement l'expression sur les réseaux sociaux via différents memes. Souvent, le message « to the moon » s'accompagne d'un émoji en forme de fusée.

Tokenisation
La tokenisation désigne le processus de numérisation d'un actif sur un token (et plus précisément un security token). Elle permet ainsi d'attribuer à différentes personnes des droits de possession ou d'utilisation de cet actif et d'échanger ses tokens en pair-à-pair sur une blockchain. Le phénomène de tokenisation pourrait à terme intervenir sur tout type de biens et d'actifs : immobilier, mobilier, titres financiers, mais aussi œuvres d'art et autres objets de valeur, brevets, crédits, droits d'auteur, matières premières... L'avantage de la tokenisation est d'augmenter sensiblement la liquidité des actifs.

Trilemme des blockchains
Le trilemme des blockchains est une limite mise en avant par Vitalik Buterin sur la base des observations des premières générations de blockchain. Pour l'instant, il semblerait impossible de parvenir à créer un système qui assure à la fois un excellent

niveau de décentralisation, de sécurité, et de scalabilité. Les premières blockchains ont présenté d'excellents niveaux de décentralisation et de sécurité, mais de gros problèmes de scalabilité. De nouvelles solutions, en particulier les blockchains de micro-paiements comme IOTA, mettent l'accent sur la scalabilité, mais cela se fait pour l'instant au détriment de la sécurité du réseau. Le trilemme des blockchains est pour l'instant d'actualité et la priorité est désormais de trouver un compromis satisfaisant entre ces trois critères.

Triple creux

Le triple creux est une figure chartiste également appelée triple bottom reversal. Le triple creux ou triple bottom reversal est une figure de retournement haussière. Cette situation apparaît donc en fin de tendance baissière. On appelle aussi cette figure cette figure "wv". Le triple creux évolue entre une ligne de support et une ligne de résistance horizontale. La figure indique l'essoufflement du courant vendeur. Les creux sont donc de moins en moins bas. On pourra généralement prendre une position à l'achat à partir de la formation du deuxième ou du troisième creux.

Trois corbeaux

Les trois corbeaux sont une figure de renversement des chandeliers japonais. En tendance haussière ou sur des hauts niveaux de marché, ils peuvent annoncer une baisse des prix. Les trois corbeaux sont trois chandeliers noirs. Idéalement, le corps de premier chandelier est au dessus de la partie la plus haute des bougies blanches précédentes. Chaque ouverture de bougie se fait à l'intérieur du corps de la bougie précédente. Les trois chandeliers clôturent au niveau de leur plus bas.

UTXO

Le terme "UTXO" est l'acronyme de "Unspent Transaction Output" soit en français "une sortie de transaction non dépensée". Ce terme est un des piliers de Bitcoin (BTC). Il renvoie plus à un système impliquant diverses notions techniques, qu'a une définition simple.Pour faire simple, Bitcoin est un registre de transactions. La coinbase fait entrer de nouveaux bitcoins fraichement minés sur le réseaux par un "input". Au fur et à mesure des déplacements de ces bitcoins, vont se succéder tout un tas d'input pour le receveur, et d'output pour l'émetteur. Chaque wallet Bitcoin représente ainsi plusieurs inputs (les bitcoins que vous avez fait entrer sur votre wallet) et plusieurs outputs (les bitcoins que vous avez envoyé). Le montant total de bitcoins affiché sur votre wallet correspond ainsi à la somme entre la valeur positive que sont les inputs (bitcoins reçus), et la valeur négative que sont les outputs (bitcoins envoyés).Le solde de votre wallet correspond à votre UTXO : une fois la balance faite entre vos inputs & vos outputs, il vous reste (ou pas) une possibilité d'output (une possibilité de dépenser).

Uptrend

Uptrend, tendance haussière en français, désigne un marché dans lequel les cours ont tendance à s'apprécier, ce que l'on peut voir graphiquement en observant les courbes des cours.

Use case
L'expression « use case » n'est pas spécifiquement propre à la blockchain ou aux cryptomonnaies. Elle est en revanche particulièrement utilisée pour désigner les différents cas d'usage de la blockchain, qui suscitent l'intérêt de nombreuses entreprises dans tout type de secteur d'activité : supply chain, contrôle de gestion, gestion des ressources humaines, finance, commerce international… De très nombreux secteurs d'activité s'intéressent aux différents use cases de la blockchain, et souhaitent en exploiter le potentiel.

Utility token
Les utility tokens sont des tokens dédiés à l'usage d'une plateforme et ont vocation à servir de monnaie en échange des services de la plateforme. La valeur d'un utility token est corrélée à celle de la plateforme et donc au nombre d'utilisateurs ayant confiance en le produit. Les utility tokens sont les plus nombreux sur le marché, et paradoxalement, sont également les moins utiles. Peu de utility tokens apportent une vraie valeur ajoutée aux plateformes, qui acceptent généralement également des monnaies fiat pour faire croître leur nombre d'utilisateurs.

Vaporware
Un vaporware, des termes anglais signifiant "vapeur" et "marchandise", est parfois traduit par le terme "fumiciel" en français. Initialement, un vaporware désigne un logiciel dont la sortie est annoncée mais le lancement est constamment repoussé, ce qui peut rendre un projet suspect. Dans l'univers des cryptomonnaies, l'adjectif "vaporware" désigne un coin qui n'a pas de vrai projet et ne vaut donc pas grand chose. On trouve aussi les termes "shitcoin" et "scam" (arnaque). Exemples: Veritaseum, Paccoin, Fucktoken, Dimoincoin…

Vitalik Buterin
Vitalik Buterin est le co-fondateur d'Ethereum, deuxième plus grosse blockchain après celle de Bitcoin. Né le 31 janvier 1994, Vitalik Buterin est un développeur de génie de sa génération. Il est également connu pour être co-fondateur de Bitcoin Magazine. Buterin est très apprécié de la communauté crypto et fait partie des figures mythiques de l'écosystème.

Volatilité
La volatilité représente les variations du cours d'une monnaie (ou d'un autre titre) sur un période définie. Plus elle est élevée, plus on considère que le titre est risqué, puisque nous n'avons pas de garantie que sa valeur ne baisse pas significativement

dans un court laps de temps. La volatilité est très importante sur le marché des cryptomonnaies, ce qui en fait un marché risqué, mais aussi très profitable pour les bons traders.

Wall
Un wall fait référence à un très gros ordre d'achat ou de vente. On utilise le mot « wall » car l'importance de l'ordre affiche comme un mur sur l'orderbook et occupe tout l'espace disponible.

Whale
Un whale, une baleine en français, est un investisseur pesant un poids important sur un marché. Dans le monde de la cryptomonnaie, les whales sont généralement des personnes ayant investi très tôt dans le bitcoin et accumulé une quantité de cryptomonnaies suffisamment importante pour influencer les cours en passant une transaction.

Wallet
Un wallet, portefeuille en français, est une application qui gère vos clés privées et donc vos cryptomonnaies. Un wallet électronique offre plusieurs fonctions: afficher le solde de vos coins, créer des adresses publiques et des clés privées, envoyer et recevoir des coins... Il existe quatre types de wallets: paper wallet, hardware wallet, desktop wallet, et exchange wallet.

Weekly
Le weekly, hebdomadaire en français, est un résumé envoyé généralement le lundi par des médias ou agences spécialisées dans les marchés financiers résumant les actualités de la semaine passée et ce qui devrait se passer la semaine de l'envoi.

Whitelist
Une whitelist, « liste blanche » en anglais, est une liste de personnes habilitées à participer à une ICO. Les organisateurs de l'ICO vous demandent de satisfaire certains critères assez faciles à atteindre (avoir une adresse e-mail valide, prouver que vous avez un wallet ETH hors exchange...) pour vous intégrer à leur whitelist, histoire de donner un côté exclusif à leur ICO.

Weak hands
« Weak hands » est un terme moqueur pour désigner les personnes qui paniquent facilement et vendent leurs cryptomonnaies très vite à la moindre rumeur négative ou dès le début d'une tendance baissière. Ce type de comportement fait souvent perdre beaucoup d'argent à leurs investisseurs, c'est pourquoi il est important d'avoir

une pleine et entière connaissance des risques du marché et de prévoir des plans de trading pour gérer son risque.

White hat / Black hat

Les termes “black hat” et “white hat” renvoient à des individus experts en sécurité informatique. Ils utilisent leurs compétences pour s’introduire dans un système informatique sans l’autorisation du concepteur. Le “white hat” désignera alors un pirate éthique, qui alerte la société de la présence d’une faille de sécurité. À l’inverse, le “black hat” sera celui qui exploitera la faille pour son intérêt personnel, en subtilisant par exemple des données pour les revendre sur Internet.

White paper

Le white paper est le livre blanc d’une cryptomonnaie. Il définit ses bases technologiques, explique son mécanisme de consensus (algorithme, récompenses) et présente éventuellement un business model et un business plan si la cryptomonnaie est un token. L’étude du whitepaper permet d’en apprendre davantage sur chaque projet, son équipe, et de se faire une opinion personnelle sur sa viabilité avant d’investir. Il s’agit de la meilleure source d’information possible pour se renseigner sur un projet de cryptomonnaie.