CRYPTO FORTUNE

DICTIONNAIRE DE LA CRYPTOMONNAIE



CRYPTO FORTUNE Tome 1 DICTIONNAIRE DE LA CRYPTOMONNAIE

Iniko Kodjo Helle



POSITIVE INTERNET SOLUTION

Mieux Faire pour le Futur Maintenant!

Email : contact@positiveinternetsolution.com

Copyright 2021... All rights reserved

Toute reproduction, conservation en mémoire dans un système d'extraction ou transmission sous une forme ou par quelque procédé que se soit, est permise par l'auteur, à condition de ne pas modifier le contenu. Cet Ebook et tout son contenu sont protégés par les lois sur la protection des droits d'auteurs et de la propriété intellectuelle de tout pays. L'auteur se réserve le droit de réclamer des dommages et intérêts si ces termes ne sont pas respectés.

© Iniko Kodjo Helle 2021

Conception graphique de la couverture :

B&D GRAPHIC

SOMMAIRE

AVANT PROPOS	5
INTRODUCTION	6
MOTS COMMENÇANT PAR :	
A	7
B	9
C	13
D	17
E	22
F	25
G	27
H	28
I	29
К	30
L	30
M	32
N	35
O	36
P	37
R	39
S	40
Т	45
U	47
V	47
W	48
Υ	49
RESSOURCES UTILES	
GAGNEZ DU TEMPS ET DE L'ARGENT AVEC CRYPTO FORTUNE Tome 2	53
MA STRATEGIE POUR VOUS FAIRE GAGNER 2000€/MOIS	57

AVANT PROPOS

Toutes les informations contenues dans cet ouvrage ne sont que des avis personnels de son auteur et ne constituent en aucun cas des conseils en investissement. La décision d'utiliser votre argent et la manière de l'investir ou non sur le marché des cryptomonnaies vous revient à vous seul. Il est fortement recommandé de toujours faire ses propres recherches avant d'investir n'importe quel montant dans un actif numérique.

Les cryptomonnaies sont des actifs très volatils et peu réglementés par nature. Le prix du bitcoin ou de n'importe quelle altcoin peut tomber même à 0\$ à tout moment et les plateformes pour la gestion de portefeuilles, l'achat et la vente de cryptomonnaies peuvent également fermer sans que vos investissements ne vous soient retournés. C'est exactement ce qui montre l'aspect cruel de ce marché.

Sur ce même marché, vous n'avez pas besoin d'investir beaucoup d'argent avant de repartir avec une grosse fortune de plusieurs milliers d'euros. Passionnant n'est-ce pas ? C'est pourquoi vous ne devez investir que ce que vous pouvez vous permettre de perdre sans que cela n'affecte vos finances. C'est la règle d'or pour ce marché et il est important de comprendre cela.

INTRODUCTION

Tout comme n'importe quel domaine, la technologie *blockchain* se structure également. **CRYPTO FORTUNE Tome 1** est un glossaire des nouveaux mots fréquemment utilisés dans l'univers des cryptomonnaies et de tout l'écosystème de la *blockchain*. Des mots et des expressions classés par ordre alphabétique et expliqués en français facile.

Découvrez à partir de la page 58, cette stratégie basée sur l'affiliation, qu'utilisent ces internautes pour gagner 100€ par jour sans investissement dans les cryptomonnaies et que vous aussi vous pouvez aisément appliquer.



Adresse

Une adresse correspond à une clé publique qui permet de recevoir des cryptomonnaies ou d'en envoyer. Cette clé publique peut prendre la forme d'une suite de lettres et de chiffres ou d'un QR code. On pourrait comparer cette adresse à un RIB/IBAN pour les monnaies classiques ou à une adresse email pour l'envoi de mails.

À titre d'exemple, la toute première adresse bitcoin ayant reçu des bitcoins : 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

Airdrop

C'est une pratique qui consiste à distribuer gratuitement une cryptomonnaie à un tiers. Il n'y a donc aucune compensation financière réclamée. En contrepartie, le bénéficiaire doit respecter certains engagements, qui diffèrent d'un projet à l'autre. Ceux-ci peuvent se traduire par l'adhésion à un groupe sur les réseaux sociaux, l'ajout d'une channel Telegram, ou encore le partage d'une actualité.

Pour une structure professionnelle, l'intérêt de l'Airdrop est multiple. Il s'agit d'une opération de communication qui permet de promouvoir son activité tout en veillant à fidéliser des clients et prospects. Fonctionnant sur le principe de la récompense, le système peut être appliqué de manière ponctuelle ou à intervalles réguliers. À l'occasion d'un lancement de produits ou d'un changement de cryptomonnaie, par exemple.

All-in

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

Altcoin (Monnaie Alternative)

Altcoin est l'abréviation pour « *Alternative Coin* ». Une altcoin désigne toutes les cryptomonnaies autre que le Bitcoin.

AMA (Ask me anything (en français, demandez-moi n'importe quoi).

C'est une expression utilisée sur les forums internet lors des discussions au cours desquelles les acteurs confirmés de la cryptosphère répondent aux diverses questions qui leur sont posées par les débutants.

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

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

Analyse fondamentale

L'analyse fondamentale s'oppose à l'analyse technique (l'analyse des graphiques de cours financiers) et recherche la valeur intrinsèque d'un protocole de finance décentralisée.

APY (Annual Percentage Yield)

C'est le retour sur investissement en réinjectant les intérêts gagnés au fur et à mesure. C'est de l'intérêt composé.

APR (Annual Percentage Rate)

C'est l'intérêt brut, gagné sur un an, comme le livret A. C'est de l'intérêt simple.

Arbitrage

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

Swissborg¹ est une plateforme d'exchange qui aide les investisseurs qui désirent faire de l'Arbitrage.

Arbre de Merkle

L'arbre de Merkle présente une structure spécifique pour recouvrir un ensemble de données. Dans le domaine de la cryptomonnaie, il s'agit essentiellement de transactions issues de la blockchain. Composé de blocs, il permet de simplifier l'accessibilité des données, en vue de vérifier leur intégrité. Le cas échéant, il est ainsi possible d'autoriser une transaction sur la base du profil de l'émetteur, sous réserve de fonds suffisants.

L'arbre de Merkle évite la consultation complète de la base de données. Il n'est donc pas nécessaire de la télécharger dans son entièreté, mais uniquement la «branche» que l'on souhaite parcourir. En parallèle de la cryptomonnaie, le principe s'applique à d'autres usages informatiques. C'est notamment le cas de la gestion de fichiers en open source de type ZFS, la cryptographie, ainsi que les réseaux dits « pair-à-pair ».

ASIC (Application Specific Integrated Circuit)

Ce sigle signifie Application Specific Integrated Circuit. Ce sont des machines dédiées à une tâche unique. Dans le cadre des cryptomonnaies, les ASICs servent à résoudre un algorithme de minage comme le SHA-256. Pour être plus précis, ce sont des équations contenues dans l'algorithme qui sont résolues.

Ask

L'ask correspond à l'offre du marché (en rouge sur le carnet). C'est le prix auquel les vendeurs souhaitent vendre une cryptomonnaie donnée.

¹ https://swissborg.com/

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

ATH: prix le plus haut jamais atteint par une cryptomonnaie **ATL:** prix le plus bas jamais atteint par une cryptomonnaie

Atomic Swaps

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

Authentification à double facteur (2FA)

C'est un processus de sécurité par lequel l'utilisateur fournit deux modes d'identification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique/virtuel, comme une carte ou une application mobile, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.

Autonomous Money Pile ou AMP

Inventé par YFBETA, c'est un système qui gagne de l'argent tout seul, comme une intelligence artificielle. Pour se faire, le programme réinvestit une partie de l'argent généré grâce à la liquidité des humains dans son protocole, pour en tirer des bénéfices. Une partie de ses bénéfices est réinjecté dans le *vault* et l'autre partie sert à *burn* (brûler, supprimer) des tokens pour maintenir le prix du jeton. C'est une sorte de pile à l'infini.

B

Bear Market

Marché à tendance baissière.

Bid

Enchère, offre d'achat correspond à la demande du marché (en vert sur le carnet). C'est le prix auquel les acheteurs souhaitent acheter une cryptomonnaie donnée.

BIP (Bitcoin Improvement Proposal)

Acronyme pour désigner « *Bitcoin Improvement Proposals* », le BIP se présente sous la forme d'un document technique qui expose une proposition d'amélioration pour le bitcoin. Son contenu concerne tous les aspects de cette cryptomonnaie. Il peut alors s'agir du système de communication pour effectuer les transactions, de l'optimisation de l'interface, ou de la réglementation d'utilisation.

Le BIP est nécessaire, car le bitcoin s'appuie sur le principe de l'open source. À défaut d'une autorité centrale, le procédé permet de gérer au mieux le développement et le bon fonctionnement de la cryptomonnaie. Sur la base d'un argumentaire et d'une explication détaillée, la communauté décide de l'application ou du rejet des suggestions avancées.

Bitcoin

Le Bitcoin est une monnaie électronique décentralisée conçue en 2009 par un développeur non identifié utilisant le pseudonyme de **Satoshi Nakamoto**. Quand on l'écrit **B**itcoin, il s'agit du protocole ou réseau. Quand on l'écrit **b**itcoin, il s'agit de la cryptomonnaie.

Symbole monétaire officiel : **B**

Sigles utilisés par les plateformes d'échanges : BTC et XBT

Bitcoin ATM

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

Bitcoin Core

Lancé en 2009, Bitcoin Core est un logiciel conçu pour accéder au réseau bitcoin. Il s'agit d'un client de type « pair-à-pair » disponible en open source. À partir des nœuds du réseau, il contrôle également l'état de transactions, et sert aux activités de minage liées à la cryptomonnaie. La communauté a réalisé de nombreuses mises à jour afin d'améliorer les fonctionnalités de Bitcoin Core. Cela vaut, entre autres, pour effectuer des transactions sans forcément passer par la blockchain originelle.

À noter que l'intégration d'un wallet permet de stocker la cryptomonnaie. Ce qui évite la perte ou le blocage des bitcoins. Son usage nécessite le téléchargement et l'installation du logiciel sur un poste dont la capacité de stockage minimale est de 200 Go.

Bitcoin Maximalist

C'est un terme qui désigne les personnes qui ont investi dans la cryptomonnaie alors que sa valeur pécuniaire était faible, voire nulle. Ils effectuent uniquement leurs transactions à l'aide du bitcoin, et promeuvent ses avantages, sans nécessairement faire preuve d'objectivité sur ses limites ou ses inconvénients.

Le maximalisme valorise la dominance du bitcoin sur le marché par rapport à d'autres cryptomonnaies. En complément de l'utilisation exclusive du bitcoin, une partie de la communauté Bitcoin Maximalist met également en œuvre des moyens de substitution pour imposer la cryptomonnaie aux autres usagers. Cela passe, entre autres, par une tentative de monopolisation des blockchains. La limite légale de ces méthodes se heurte alors au libéralisme inhérent au domaine des cryptomonnaies. Il s'agit néanmoins d'une pratique non généralisée à l'ensemble du mouvement maximaliste.

BitPay

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

Bloc

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

Blockchain (Chaîne de Blocs)

La blockchain est une liste complète de tous les blocs de transactions complétés depuis le début du Bitcoin. Afin de renforcer la sécurité du système, la blockchain a été conçue de sorte que chaque bloc de transactions contienne le *hash* produit à partir du bloc précédent.

La blockchain est une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente, et fonctionnant sans organe central de contrôle. Par extension, la blockchain désigne une base de données sécurisée et distribuée (car partagée par ses différents utilisateurs), contenant un ensemble de transactions dont chacun peut vérifier la validité. La blockchain peut donc être comparée à un grand livre comptable public, anonyme et infalsifiable.

Bloc Genesis

Premier bloc d'une blockchain. La fonction du bloc Genesis est primordiale : celui-ci permet, en effet, de créer une fondation solide qui garantit l'harmonisation de l'ensemble de la chaîne de blocs de cryptomonnaie générés au cours du temps. En ce sens, chaque bloc de genèse sert à maintenir la communication entre deux nœuds (même si chaque nœud a son propre bloc initial). L'ensemble forme alors un immense réseau, dont toutes les parties sont ancrées à la même origine.

Si on compare une cryptomonnaie à une pyramide de blocs, le sommet de l'édifice serait le bloc de genèse qui présiderait l'ensemble des blocs. Ainsi, peu importe le nombre de liens générés, ils auraient tous la même source.

Block height

Le terme "block height" peut se traduire par "instrument de mesure de la hauteur" et, plus spécifiquement, de l'écart de création temporel, entre deux blocs composant une blockchain. Dans l'univers de la blockchain, le block height permet, en assignant une numérotation à chaque bloc créé, de situer le moment de création d'un bloc par rapport à un autre, ou par rapport au bloc originel.

En ce qui concerne la blockchain bitcoin, par exemple, le premier bloc de transactions, nommé "bloc genesis", a été créé le 3 janvier 2009 à 18h15. Sa hauteur (height) était de zéro, ce bloc étant le premier. Dans le cas de la blockchain bitcoin, toujours, l'écart de création entre deux blocs par les mineurs est d'une dizaine de minutes. Mais ce décalage n'est pas universel et varie selon les

blockchains, à commencer par les blockchains de cryptomonnaies alternatives au bitcoin (altcoins).

Bloc orphelin

Le bloc orphelin est un bloc généré par l'activité minière, mais ne faisant pas partie d'aucune blockchain. Initialement, les blocs orphelins étaient des blocs correctement résolus, mais dont l'ascendance complète n'était pas connue. De ce fait, faute de bloc parent associé, ces blocs ne pouvaient pas être validés dans la blockchain.

Si ce phénomène était encore courant dans les premières versions du logiciel Bitcoin, il est depuis 2015 et la version v.0.10 impossible d'en voir survenir dans la chaîne de blocs générés par l'activité minière. Par ailleurs, ne pouvant pas entrer dans la blockchain, ces blocs sont entreposés dans un pool spécifique : le pool de blocs orphelins.

À noter que, dorénavant, le terme de "bloc orphelin" sert également à désigner les blocs qui sont générés presque simultanément par deux mineurs. Le bloc qui aura la "preuve de travail" (PoW) la plus petite sera alors rejetée de la chaîne.

Block Reward (Récompense de Bloc)

Récompense reversée par la blockchain lorsqu'un bloc est trouvé. Contrairement à ce que l'on pourrait croire, trouver un bloc n'apporte pas une unité de la cryptomonnaie en récompense mais une valeur qui est initialement fixée par les développeurs de la cryptomonnaie et ajustée dans le temps. Pour le Bitcoin par exemple, cette valeur est actuellement de 6,25 bitcoins par bloc et sera divisée par 2 lors du halving du Bitcoin en 2024. Elle passera donc à 3,125 bitcoins par bloc au prochain halving.

Bottom

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

BTFD (crypto):

Acronyme de "Buy the Fucking Dip!", l'expression est surtout utilisée lorsque le marché d'une cryptomonnaie s'effondre à la suite d'un mouvement de peur ou de panique et que les investisseurs ont l'opportunité unique d'acheter cette devise avec un rabais intéressant ou à un prix très inférieur à sa valeur réelle ou supposée.

Le BTFD peut relever d'une stratégie réfléchie visant à tirer profit d'une future hausse de la devise, mais il peut se comprendre aussi comme un cri de ralliement de traders qui font face à une situation de crise et espèrent des jours meilleurs, une attitude pour démontrer leur confiance dans l'avenir de la monnaie et rassurer les troupes.

L'expression est devenue populaire dans le monde du trading au moment de la crise des subprimes. De nos jours, elle s'emploie beaucoup par les investisseurs en crypto qui voient les devises subir de fortes fluctuations d'une période à l'autre et peuvent réaliser une plus-value en achetant une monnaie lorsqu'elle est au plus bas.

Bug bounty (prime aux bogues)

C'est un programme de récompenses proposé par de nombreux sites web, développeurs de logiciel, réseaux sociaux et maintenant des plateformes d'échange de cryptomonnaies, de la finance décentralisée (DeFi) qui offre des récompenses aux personnes appelées des *whyte hackers* (des pirates gentils) qui découvrent d'éventuels défauts de conception. Ces programmes permettent aux développeurs de la plateforme de découvrir et de corriger des failles de sécurité avant que les hackers malveillants et le grand public en soient informés, évitant ainsi des attaques informatiques.

Le site web Immunefi² publie régulièrement les plateformes et projet DeFi qui utilisent le *bug bounty* afin de se protéger contre les piratages informatiques.

Bull Market

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

Bullrun

Période dynamique de fortes hausses, voire d'euphorie sur le marché des cryptomonnaie.

Burn

Le fait de détruire des tokens d'une cryptomonnaie.

Buy wall (crypto)

Un « wall » est la représentation d'un mur sur le carnet d'ordre de la plateforme d'échange d'une cryptomonnaie, sur laquelle sont effectués les ordres de vente et d'achat. On parle de « buy wall » dès lors qu'un volume important d'achats a été effectué au même prix par un utilisateur, ou lorsque plusieurs investisseurs effectuent simultanément des achats d'une devise au même prix.

CBDC (Central Bank Digital Currencies)

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

_

² https://immunefi.com/

CDP (Collateralized Debt Position)

Une position de dette garantie (CDP). Elle permet par exemple la génération de stablecoin *DAI* contre des garanties (notamment en ETH, WBTC ou USDC) que vous verrouillez dans un CDP jusqu'à ce que vous remboursiez le DAI que vous avez généré.

CEX

Acronyme anglais de Centralized Exchange ou plateforme centralisée en Français.

Exemple: Binance³; Coinbase⁴; Kraken; CEX.IO⁵; FTX⁶

CFD

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

Chart

Il s'agit des graphiques des cours/prix des cryptomonnaies.

Clé privée

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

Clé publique

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

Cloud mining

Le cloud mining est la location d'une quantité de puissance de calcul dans une ferme de minage située à distance. De cette manière, un mineur peut participer au minage d'une cryptomonnaie, sans pour autant posséder le matériel nécessaire, très coûteux et volumineux. En contrepartie, le mineur règle une rente qui prend la forme d'une location classique.

³ https://www.binance.com/fr/register?ref=ZXS1S4M0

⁴ https://www.coinbase.com/join/helle_51

⁵ https://cexio.page.link/cxHf

⁶ https://link.blockfolio.com/9dzp/aaf88480

En recourant au cloud mining, les investisseurs prennent donc un risque bien plus mesuré que s'ils faisaient l'acquisition d'un set up de minage (même minimaliste). Dans le même temps, ils dégagent également des bénéfices réguliers. De ce fait, il s'agit d'une porte d'entrée raisonnable dans le monde des cryptomonnaies, en particulier pour les mineurs au capital plus que modeste. Plusieurs sociétés proposent d'ailleurs des offres de cloud mining avec des tarifs adaptés à toutes les bourses.

Coinbase

Champ spécial utilisé comme unique entrée pour les *transactions coinbase*. Cela permet de récupérer la récompense de minage d'un bloc bitcoin et permet d'inclure jusqu'à 100 bytes de données.

Coinbase Transaction

La première transaction dans un bloc. Toujours créée par un mineur, elle inclut un seul coinbase.

Collateral

On appelle collatéral (en anglais « collateral ») l'ensemble des actifs, titres ou liquidités, remis en garantie au créditeur. En cas de défaillance du débiteur, le créditeur a le droit de conserver le collatéral afin de se dédommager de la perte financière subie.

Cold storage

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

Colored coins

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

Confirmations

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

Consensus

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

Copy Trading/Social Trading

Le Copy Trading et le trading social consistent à copier simplement des traders professionnels qui mettent à disposition leurs compétences et surtout leurs meilleures stratégies de trading.

Correction

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

CPU

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

Crypto-actif

Ensemble des actifs numériques émis et échangeables sur une blockchain (cryptomonnaies et tokens).

Crypto-anarchie

Le Crypto-anarchie ou Crypto-anarchisme est la réalisation dans le cyber-espace d'une forme d'anarchie par l'usage de la cryptographie en offrant aux individus une totale liberté d'échange, tout en garantissant leur anonymat et le respect de leur vie privée.

Cryptographie

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

Cryptographie asymétrique

C'est un procédé qui intègre deux clés de chiffrement : une clé publique et une clé privée. Par convention, la clé de chiffrement du message est appelée clé publique (et peut-être communiquée sans restriction aucune), et la clé de déchiffrement du message est appelée clé privée. Cette dernière ne doit être communiquée sous aucun prétexte.

Avec une clé publique, l'expéditeur code dans un algorithme de chiffrement un message ou une énigme qui ne pourra être, au final, décodé ou résolu que par le destinataire détenteur d'une clé privée, donnée en entrée d'un algorithme de déchiffrement. Dans l'écosystème bitcoin, la cryptographie est utilisée pour protéger les fonds d'un détenteur de cette cryptomonnaie, pour encrypter le porte-monnaie, mais aussi pour préserver l'intégrité de la blockchain bitcoin.

Cryptojacking

Le cryptojacking (également nommé « minage de cryptomonnaie malveillant ») est une menace qui s'insinue dans un ordinateur ou dans un appareil mobile, pour détourner les ressources de la machine afin de miner des cryptomonnaies (à l'insu du possesseur desdits appareils).

Menace naissante dans le monde des nouvelles technologies, le cryptojacking peut se déclencher via des navigateurs web, pour ensuite corrompre tous types d'appareils (des ordinateurs de bureau aux smartphones, en passant par les ordinateurs portables). Les appareils infectés sont donc surexploités à l'insu de leur propriétaire, ce qui cause évidemment des dégâts matériels. En agissant de la sorte, les hackers tirent donc profit de matériels informatiques appartenant à des tiers, ce qui les dispense d'investir dans du hardware, pour miner des cryptomonnaies.

Cryptomonnaie

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

Cypherpunk

Mot-valise forgé par la hackeuse et auteure américaine **Jude Milhon** en 1992 (à partir des termes « cypher » pour cryptage et « punk » pour rebelle ; ce qui crée une assonance avec le terme de « cyberpunk »). Le cypherpunk est le membre d'un groupe informel de personnes luttant pour le respect de la vie privée sur Internet, en faisant notamment l'usage de la cryptographie. Ce mouvement a débuté en même temps qu'émergeait l'industrie informatique, c'est-à-dire dans les années 1970.

Avec la croissance rapide de l'ARPANET, dans les années 1980, les cypherpunks gagnèrent de l'ampleur et introduisirent la cryptographie (qui était, alors, surtout utilisée par des militaires) dans le champ de l'Internet mondial. Bien qu'étant centré sur le domaine technologique, le milieu des cypherpunks a également été un environnement propice à des idées anarcho-capitalistes, faisant notamment l'apologie de la "crypto-anarchie".



DAI (jeton)

C'est un *stablecoin* qui fait office d'emprunt contracté avec Ethereum (des ETH peuvent donc être convertis en DAI). Comme le suggère le terme de « stablecoin », l'intérêt de cette monnaie décentralisée est de garder une valeur stable. De cette manière, elle peut donc servir de couverture lorsque le marché est baissier. Basé sur la blockchain d'Ethereum, ce stablecoin créé par MakerDAO est en outre décentralisé.

De type ERC-20, ce token est conçu de sorte à préserver sa valeur indexée sur le dollar américain. Ainsi, chaque DAI a la valeur de 1 dollar. Il permet, de ce fait, de transférer des actifs (par-delà les frontières) de manière rapide et sans frais annexes. Son ajustement est également dynamique, ce qui lui permet de maintenir son ancrage en dollars. Les possesseurs du jeton DAI peuvent même utiliser un mécanisme appelé « taux d'épargne DAI » leur permettant d'obtenir un rendement très stable.

Dapps

Les dApps sont des applications décentralisées qui fonctionnent sur Ethereum et qui sont permises par les *smart-contracts*.

DAO (Organisation décentralisée autonome)

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

Dark pool

Pratique visant à permettre à un acteur important dans une cryptomonnaie de réaliser une transaction anonyme sur une plateforme spécifique, sans que le reste du marché en soit aussitôt informé, dans le but d'éviter un inévitable mouvement baissier ou haussier sur le cours de la devise. Cela permet à cet acteur de nouer une grosse transaction à l'achat ou à la vente sans que cela affecte la valeur de la cryptomonnaie en sa défaveur.

Si un investisseur institutionnel, un gros trader ou une banque par exemple, décide de vendre toute ou partie de son stock pour encaisser une plus-value, la simple annonce publique de son retrait risquerait de faire chuter la valeur de la devise et d'impacter négativement son gain. Mais en passant par une plateforme « dark pool », ce risque est éliminé étant donné que la transaction n'est révélée au reste des détenteurs qu'après avoir eu lieu! Kraken fut la première bourse d'échange à proposer ce service dans le bitcoin en 2015. La pratique s'est beaucoup développée depuis.

Day Trading

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

Le DCA ou « Dollar Cost Averaging »

C'est une stratégie d'investissement qui consiste à acheter une cryptomonnaie pour la même somme en dollars (ou en euros) à des intervalles réguliers et programmés à l'avance. Le but de ces achats périodiques à somme identique est de réduire le risque pris, sans se fier au cours de la devise.

Cette stratégie, qui est appréciée des investisseurs de long terme, n'est pas toujours la plus rentable, mais sans doute l'une des moins risquées. En effet, dans les périodes baissières, seule une partie de l'investissement est affectée par le déclin de la devise, c'est-à-dire les derniers achats. À moins d'un effondrement, le reste de l'investissement est « prémuni » contre la volatilité.

Pour se lancer dans une stratégie de DCA, l'investisseur doit déterminer deux paramètres : la somme qu'il est prêt à investir à chaque achat et le délai entre deux transactions. L'intervalle le plus fréquent est compris entre six mois et un an.

Bitpanda⁷ et Coinbase⁸ sont des exchanges sur lesquelles il est possible de pratiquer le DCA. D'autres structures comme EPARGNE DU COIN⁹, proposent des services DCA à leurs abonnés.

DDoS (Attaque par Déni de Service)

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

Décentralisation

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

DeFi (Finance Décentralisée)

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

Déflation

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

Desktop wallet

Un desktop wallet est un programme logiciel qui permet de stocker une ou plusieurs cryptomonnaies sur un ordinateur de bureau ou sur un ordinateur portable. Connecté à Internet, le desktop wallet est aussi appelé "hot wallet", par opposition aux "cold wallets" qui sont des

⁷ https://www.bitpanda.com/en

⁸ https://www.coinbase.com/join/helle_51

⁹ https://journalducoin.com/epargne-du-coin/

dispositifs de stockage de cryptomonnaies (comme, par exemple, une simple feuille de papier) qui ne sont pas connectés à Internet.

Il existe deux catégories de desktop wallets: les clients complets (*full wallets*) et les clients légers (*lightweight wallets*). Les clients complets, à l'instar de la solution Bitcoin Core, vont télécharger l'intégralité de la blockchain bitcoin sur le disque dur de l'ordinateur qui héberge le wallet. L'ordinateur hôte devient alors un nœud complet ("*full node*") participant à la sécurisation du réseau bitcoin. Les clients légers (Exodus ou Electrum) sont, en revanche, dépendants d'une connexion à un serveur central pour accéder à la blockchain.

DevFee (Developer Fee)

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

DEX

Ce sont des plateformes d'échanges de cryptomonnaies décentralisées qui, contrairement aux plateformes d'échanges centralisées, pourront plus efficacement lutter contre les attaques informatiques. De plus, elles préservent davantage la sécurité, la vie privée et l'autonomie. La majorité des DEX (90 % des plus actives) est hébergée sur le réseau Ethereum.

En pratique, si vous souhaitez échanger de l'ETH contre du DAI par exemple, les agrégateurs vont comparer les différents taux pratiqués par les DEX, et procéder à l'échange sur celle qui propose le meilleur taux. Au final, la plateforme est une simple interface qui met en contact un acheteur et un vendeur. Pour cela, vous n'avez besoin de rien de plus qu'un identifiant, un mot de passe et un portefeuille crypto. En revanche, les DEX sont plus lentes que les plateformes d'échange centralisées, notamment en cas de fort trafic.

Exemple: Uniswap¹⁰; Pancakeswap¹¹; Binance Dex¹²

Difficulté

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

Dip

Il s'agit d'une chute brutale et éphémère du cours qui retrouve très rapidement sa valeur. Cela peut correspondre à une vente importante par une baleine. Les dips peuvent constituer

¹⁰ https://app.uniswap.org/#/swap

¹¹ https://pancakeswap.finance/

¹² https://www.binance.com/fr/register?ref=ZXS1S4M0

de bonnes opportunités pour ceux qui ont placé des ordres d'achat. L'expression *Buy The Fucking Dip* consiste à acheter les points les plus bas dans un marché haussier.

DPoS (preuve d'enjeu déléguée)

C'est un mécanisme de consensus qui permet aux détenteurs de cryptomonnaie de voter en temps réel pour des candidats qui promettent d'assurer le bon fonctionnement et la sécurité de la blockchain. Le droit de vote est fonction du nombre de jetons que possède l'utilisateur. Avec ce type de construction plus démocratique, les interactions entre les nœuds sont réduites, puisque les participants du réseau n'ont pas besoin de télécharger l'ensemble de la blockchain pour valider une transaction. Naturellement, cela se traduit par la possibilité de réaliser un grand nombre de transactions avec des validations beaucoup plus rapides (quelques secondes seulement, contre les 10 minutes avec le système de *Proof- of- Work* utilisé par le réseau Bitcoin).

Double dépense

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

Dump (Baisse du prix d'une cryptomonnaie)

Par opposition au phénomène de *pump*, le dump désigne la chute soudaine, brutale et souvent suspecte (car souvent liée à une tentative de manipulation de marché) d'un cours. Ici, celui d'une cryptomonnaie. Le dump est souvent précédé d'un pump (c'est-à-dire du gonflement artificiel à des fins spéculatives) du cours. Les plus importants de ces investisseurs sont appelés "whales" (baleines, en français), car ils détiennent d'importantes quantités de telle ou telle cryptomonnaie.

DYOR (*Do Your Own Research*)

C'est la phrase la plus répétée et la plus vénérée du monde de la blockchain et des cryptomonnaies, signifiant en français "Faire vos propres recherches".

DYOR est ce qui se rapproche le plus d'une règle d'or pour le marché des cryptomonnaies car elle est une des clés pour garantir un succès et constitue un excellent remède contre le FOMO.



ECDSA

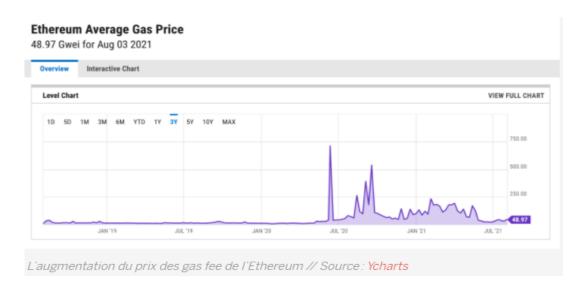
Elliptic Curve Digital Signature Algorithm est un algorithme cryptographique utilisé par Bitcoin pour s'assurer que les fonds peuvent uniquement être dépensés par leurs propriétaires.

EIP-1559 (Ethereum Improvement Proposal)

Il s'agit d'une mise à jour majeure (*hard fork*) réalisée sur la blockchain Ethereum pour de nombreuses améliorations techniques demandées depuis longtemps. Désignée sous l'appellation "London", cette mise à jour apporte également son lot de nouveautés.

Pour mieux comprendre les enjeux auxquels London doit répondre, il faut rappeler que la blockchain d'Ethereum est très utilisée, que ce soit pour les NFTs, ou pour l'exécution de contrats intelligents. Ces nombreux usages font que le nombre d'interactions sur la blockchain est élevé: on en compte entre 10 et 30 à la seconde sur Ethereum, contre entre 3 et 7 transactions par seconde sur la blockchain du bitcoin.

Seulement, la blockchain a du mal à répondre à toutes les demandes, qui sont de plus en plus nombreuses. C'est notamment pour cela que le prix des "gas fee", des frais qui s'appliquent pour chaque transaction inscrite sur la blockchain, augmente graduellement depuis des années.



Pour les mineurs, qui touchent ces gas fee en échange de la validation des transactions sur la blockchain, la montée des prix est une très bonne nouvelle. Mais pour toutes les autres personnes, et particulièrement celles qui se servent de la blockchain pour développer des applications, les gas fees sont devenus un vrai poids économique. Le problème est devenu tel que certains projets concurrents de blockchain pour contrats intelligents se sont

montés, comme Solana, Binance Smart Chain et de nombreux utilisateurs d'Ethereum ont préféré partir. Afin de remédier à ce problème, une EIP, proposition d'amélioration pour Ethereum a été déposée.

Elle prévoit de modifier le fonctionnement du montant des gas fee, jusqu'à présent calculé en fonction du nombre de transactions en cours sur la blockchain. Il sera désormais calculé selon un autre modèle. Il y aura un prix de base (appelé base fee), que les utilisateurs seront obligés de payer, et qui variera en fonction de la congestion de la blockchain, mais de manière précise et prévisible. À ce prix de base pourra s'ajouter une sorte de pourboire, que les utilisateurs choisiront ou non de payer en fonction de la rapidité à laquelle ils veulent leur transaction traitée. Certains experts estiment que le prix des transactions diminuerait ainsi de 90 %.

La mise à jour va également introduire la pratique du "coin burn" dans la blockchain. Le coin burn est une pratique qui consiste à détruire volontairement des unités de cryptomonnaies, le tout afin d'en faire augmenter la valeur.

London comprend également les EIPS suivants :

- l'**EIP 3198**, qui permettrait à certaines applications décentralisées d'utiliser une partie des frais de base au lieu de les détruire ;
- l'**EIP 3529**, qui limitera les remboursements liés aux frais de certaines applications et pour les transactions de contrats intelligents ;
- l'**EIP 3541**, qui va permettre de créer de nouveaux types de contrats intelligents en autorisant l'utilisation de séquences d'octets qui n'existent pour l'instant dans aucun contrat ;
- et l'**EIP 3554**, qui retarde la « bombe de difficulté » (qui va permettre de passer de la proof of work à la proof of stake en rendant la blockchain dure à miner) à décembre 2021.

ERC-20 (Token)

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

ERC-721 (Token)

Les tokens ERC-721 sont une catégorie de tokens Ethereum. Il s'agit de tokens non fongibles (NFT), qui sont particulièrement utilisés dans les jeux vidéo blockchain.

Ethereum

Ethereum est une plateforme, semblable à un « ordinateur mondial », sur laquelle on peut exécuter des applications sans avoir recours à un serveur centralisé. Chaque nœud de la blockchain est chargé d'une partie de l'exécution des applications présentes sur celle-ci.

A l'instar de Bitcoin qui n'a pas besoin d'intermédiaire (banque) pour échanger des unités monétaires, Ethereum offre des services qui n'ont plus besoin d'intermédiaires pour être exécutés. Ethereum vise à bâtir un Web où les intermédiaires entre les clients et les services qu'ils recherchent n'existent plus. Il serait par exemple possible de commander un chauffeur sans passer par un service comme Uber qui prend une commission à chaque trajet/transaction pour la mise en relation du client et du chauffeur. La blockchain Ethereum fonctionne avec la cryptomonnaie Ether dont le sigle est l'ETH.

Ethereum 2.0

Le passage du protocole de consensus de la *Proof Of Work* à la *Proof of Stake* sur la blockchain Ethereum. La Convergence aurait lieu avant la fin d'année 2021.

EVM (Ethereum Virtual Machine)

C'est un système utilisé par la plateforme Ethereum. Il s'agit même de la pièce maîtresse de la blockchain Ethereum. Elle permet d'une part de réaliser les calculs permettant d'établir des *smart contracts*, et d'autre part de s'assurer de leur fonctionnement et de leur mise en application effective sur la blockchain.

L'EVM a la capacité d'exécuter un grand nombre d'instructions, tout comme un ordinateur, de sorte qu'elle est particulièrement flexible lorsqu'elle procède à diverses opérations. On parle souvent du réseau Ethereum comme d'un ordinateur global, car chacun des nœuds connectés au réseau exécute une instance de l'EVM. Ce système fonctionne en échange de frais de déploiement et d'utilisation nommés *gas* (mais qui sont facturés en ethers) qui dépendent des opérations à effectuer. Le prix correspond à l'addition de tous les frais de chacune des opérations de la transaction.

Exchange (Plateforme d'Echanges)

C'est une place de marché ou l'on échange des cryptomonnaies entre elles ou contre des monnaies fiduciaires. Cela permet d'investir ou de spéculer sur le cours des cryptomonnaies.

Exit scam

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



Faucet (Robinet en français)

C'est un site Internet ou une application mobile qui récompense ses visiteurs ou ses utilisateurs en les "rémunérant", c'est-à-dire en leur versant des tokens ou des satochis (la plus petite unité utilisée dans le protocole bitcoin), en contrepartie du temps passé et des actions réalisées.

L'internaute qui souhaite ainsi gagner de petites fractions de bitcoins et d'altcoins (car il existe des faucets tout autant pour le bitcoin que pour des cryptomonnaies alternatives) devra au préalable effectuer des micro tâches, consistant par exemple à remplir un *captcha*, fournir une adresse e-mail, répondre à un quizz, regarder des publicités en ligne, participer à un sondage ou bien encore éliminer des créatures ou des personnages dans un jeu en ligne.

Pour être payé de manière sécurisée et anonyme, l'internaute devra, dans un premier temps, créer un porte-monnaie qui accueillera les micro-paiements provenant du site faucet. Pour la petite histoire, le tout premier bitcoin faucet, dénommé *The Bitcoin Faucet*, fut créé par un certain **Gavin Andresen** en 2010. Il distribuait, à cette époque où le bitcoin ne valait encore que 0,08 dollar, 5 bitcoins par personne.

Aujourd'hui, la quantité et la fréquence des satoshis distribués sur les sites ou les apps faucet varie en fonction de l'évolution du cours du bitcoin. Le faucet est un moyen ludique, bien que parfois chronophage, de sensibiliser le grand public au bitcoin, et plus largement au monde des cryptomonnaies. Pour ces sites et applications, qui vivent le plus souvent de la publicité ou proposent des services liés aux cryptomonnaies, "distribuer" ainsi des fractions de bitcoins ou d'altcoins est aussi un moyen d'optimiser et de développer une forte audience autour de leurs activités. Quelques exemples de sites bitcoin faucet: Freebitcoin, BitcoinAliens.

Fees (Frais)

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

Ferme de Minage

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

Fiat (Monnaie Fiduciaire)

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

Flash loan

Emprunt instantané sans risque de contrepartie, qui ne demande aucune garantie, à condition que le montant soit emprunté et remboursé dans une seule et même transaction sur Ethereum. Initialement utile aux développeurs, il a été popularisé par certains traders pour utiliser l'arbitrage avec de grosses sommes sans avoir à fournir d'actifs en garantie.

FOMO (Fear Of Missing Out)

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

Fongibilité

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

Forgeur

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

Fork

La création d'une version alternative de la blockchain. La cause de cette bifurcation peut être soit malveillante, soit accidentelle suite à un bug ou bien encore intentionnelle quand les développeurs décident d'introduire de nouvelles fonctionnalités. La version la plus longue de la blockchain devient la version principale.

FUD (Fear, Uncertainty and Doubt)

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

FUDster

A l'instar du terme "hodl", le mot "*FUDster*" appartient au champ lexical argotique des cryptomonnaies. Ce mot désigne en premier lieu les détracteurs des cryptomonnaies qui diffusent intentionnellement, pour certains de fausses informations ou des prophéties apocalyptiques dans les médias, sur les forums (comme *Reddit*) ou sur les réseaux sociaux, de manière à faire baisser les cours des cryptomonnaies (à commencer par celui du bitcoin). Ou à

tout le moins à éroder la confiance de ceux qui en détiennent, et surtout celle des détenteurs les moins aguerris.

G

Gas

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

Gossip Protocol

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

GPU (Graphical Processing Unit)

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

Gram

Projet de cryptomonnaie du réseau social Telegram. Le projet de cryptomonnaie de la messagerie cryptée est abandonné ce 13 Mai 2021. C'est **Pavel Durov**, le fondateur qui l'a annoncé sur son compte Telegram. D'après le dirigeant, cet abandon est dû à l'opposition de la justice américaine et du gendarme financier US (la Sec).

« Imaginez que plusieurs personnes rassemblent de l'argent pour construire une mine d'or et plus tard diviser l'or extraite! ». Ensuite, un juge vient dire aux constructeurs de la mine : « Beaucoup de gens ont investi dans la mine d'or parce qu'ils recherchaient des profits. Et ils ne voulaient pas cet or pour eux, ils voulaient le vendre à d'autres. A cause de cela, vous n'êtes pas autorisés à leur donner de l'or », narre Pavel Durov, qui a utilisé l'image de la mine pour désigner la blockchain TON et l'or pour le gram, la cryptomonnaie qui aurait dû en découler.



Hachage

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

Halving

On parle de halving lorsque la récompense de minage d'une cryptomonnaie est divisée par deux. Cet événement est programmé à l'avance dans le code de la monnaie et se déclenche automatiquement lorsqu'un certain nombre de blocs ont été minés.

Par exemple pour le Bitcoin : La prime de minage est divisée par deux tous les 210 000 blocs de transactions minés. Les premiers mineurs gagnaient 50 BTC par bloc généré, puis cette valeur est passée à 25 BTC en 2012 et à 12,5 BTC en 2016. Le dernier halving était intervenu le 12 Mai 2020 où la récompense des mineurs est passée à 6,25 bitcoins par bloc miné.

Hard Fork

Séparation de la chaîne de blocs (split) en deux parties pouvant aboutir à la création de deux monnaies distinctes mais avec un historique commun. Un hard fork très connu est celui de l'ETC pour créer l'ETH, suite à un désaccord de vision sur l'immutabilité de la blockchain.

Hardware wallet

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

Hashrate

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

Hodl

Ce terme, devenu un véritable phénomène sur la Toile, provient d'une faute de frappe réalisée par un détenteur de bitcoins dans un message posté sur BitcoinTalk (un forum spécialisé dans le Bitcoin. Découvrez sa signification!

Sans parler d'acte fondateur dans la jeune histoire du bitcoin, l'apparition inopinée du terme "hodl" et le succès qui s'en est suivi tiennent de ces bugs révélateurs des pratiques d'un

écosystème. Petit retour en arrière : le 18 décembre 2013, à la suite d'un énième crash du cours du bitcoin, **GameKyuubi**, un détenteur de cette cryptomonnaie poste sur un forum spécialisé un message qui fera date. **GameKyuubi** se trouve dans un état d'ébriété avancé qui le conduit à faire une faute de frappe dans l'intitulé de son message. Au lieu d'un banal "I'm holding" (Je garde mes bitcoins, pas question de les vendre), il tape (en lettres majuscules) "I AM HODLING".

Cette formule, depuis devenue un "mème", c'est-à-dire un véritable phénomène sur Internet, fait désormais partie de l'argot du bitcoin pour signifier que l'on conserve sa cryptomonnaie et que l'on sait résister à la pression provoquée à intervalles irréguliers par la chute du cours du bitcoin. Car, non content d'avoir posté un message agrémenté d'une jolie faute de frappe, **GameKyuubi** théorisait, dans le corps dudit message, le pourquoi du comment qui l'amenait à ne pas vendre ses bitcoins.

Avec cette conclusion presque imparable: dans un marché aussi agité que celui du bitcoin, les seuls acteurs qui doivent vendre en cas de grosses secousses sont les plus perspicaces (voire les spécialistes du Day Trading) et certainement pas des néophytes et/ou de nouveaux entrants (comme lui). En clair, aujourd'hui, le terme "hod!" symbolise un investissement sur le long terme, la confiance des détenteurs de bitcoins dans cette cryptomonnaie et, surtout, l'espoir qu'ils caressent que son cours finisse toujours par remonter.

Hold

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

Hot storage

On parle de *hot storage* pour désigner un type de stockage de données numériques généralement connecté à d'autres ordinateurs, réseaux ou Internet.

ICO (Initial Coin Offering)

Une ICO (Initial Coin Offering) est une méthode de distribution de tokens via une levée de fonds. Elle est utilisée pour le lancement de projets liés aux cryptomonnaies et à la blockchain. Lors d'une ICO, les investisseurs peuvent acheter des tokens, ce qui est similaire au fait d'acheter des parts dans une société classique. Cela permet au projet de lever des fonds, et cela permet aux investisseurs de prendre part au projet et de spéculer sur sa future valeur.

Interopérabilité

Le terme interopérabilité désigne le fait que des systèmes informatiques ou téléphoniques puissent s'adapter afin de collaborer avec d'autres systèmes indépendants, afin de créer un réseau et de faciliter le transfert de données.

Synonyme de compatibilité, cette capacité permet de faciliter la création d'un réseau et le transfert de données provenant de programmes différents. Les Oracles sont des programmes informatiques qui permettent d'interagir entre la blockchain et le monde extérieur pour tirer au sort les gagnants d'un pari sportif, par exemple.

K

Know Your Customer (KYC)

C'est le nom donné aux procédures de vérification utilisées par les institutions financières. Ce terme englobe toutes les demandes de justificatifs lors de la souscription du contrat, des transactions ou de la clôture du compte sur une plateforme d'exchange centralisée.

L

Lambo

Il s'agit d'un "mème". Tous les traders en cryptomonnaies s'achèteront une Lamborghini lorsqu'ils seront riches.

Last

Sur un exchange, cela désigne généralement le dernier prix auquel a été échangé une cryptomonnaie donnée.

Laszlo Hanyecz

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

Launchpad

Le Launchpad Binance a été lancé à la fin de l'année 2017. Il permet aux nouveaux projets innovants de se faire connaitre sur la plateforme et de leur donner une première impulsion sur Binance via un initial exchange offering (IEO).

En effet, grâce aux possibilités de staking du launchpad, de nouveaux utilisateurs récoltent des cryptomonnaies encore méconnues, renforcent la confiance dans cette monnaie et en parlent, ce qui permet aussi une bonne impulsion marketing pour ces projets.

Launchpool

Produit de la DeFi sur la plateforme d'exchange Binance qui permet à ses utilisateurs de gagner des tokens en bloquant les jetons natifs BNB et BUSD de la plateforme.

Levier

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

Lightning network (Réseau éclair)

Le lightning network ou réseau éclair est un projet datant de 2013 et qui consiste à ajouter une surcouche au-dessus de la blockchain Bitcoin. Ce réseau permet notamment de réaliser des paiements instantanés en bitcoin contre environ 10 minutes sans la surcouche (avec le procédé du minage). Le lightning network permet aussi de réduire les commissions sur le bitcoin.

Limit Buy / Limit Sell

Ordre placé par un investisseur qui souhaite acheter/vendre des cryptomonnaies à un prix fixé à l'avance.

Liquidity provider

Un fournisseur de liquidité. Acteur financier qui vient alimenter un pool de liquidité dans le cas d'un DEx, et est généralement rémunéré par les frais sur chaque échange.

Liquidity pools ou pools (piscines) de liquidités

Ce sont des programmes dans lesquels les utilisateurs mettent à disposition leurs fonds pour permettre l'échange de tokens dans des plateformes de swap, comme sur Uniswap¹³. Les utilisateurs gagnent ensuite les frais générés sur le pool.

Long

Faire un long consiste à miser à la hausse du cours en utilisant le Margin Trading. C'est-àdire emprunter de l'argent à un instant t pour acheter une cryptomonnaie, en espérant que le prix augmente afin de rembourser les montants empruntés tout en dégageant un profit.

¹³ https://app.uniswap.org/#/swap

Luck (Mining)

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



MakerDAO

C'est une plateforme apparue fin 2017 et qui est gérée sur Ethereum par le biais de *smart contract. MakerDAO* a mis en place deux tokens spécifiques. D'une part, le Dai (DAI), un stablecoin unique en son genre, puisque c'est un token dont la valeur ne varie pratiquement pas (1 DAI équivaut à 1 dollar, sans fluctuation ou presque). D'autre part, le *Maker* (ou MKR), un token permettant à ses possesseurs de voter, et donc de participer à la gouvernance du projet *MakerDAO*.

Cette gouvernance permet de gérer des paramètres aussi variables que les taux d'intérêt, le ratio ou les pénalités de liquidation, par exemple. *MakerDAO* permet aussi de réaliser des prêts et des économies sur la blockchain Ethereum. Le protocole *Maker* est nécessaire au maintien de la stabilité du *DAI*, puisque c'est lui qui garantit que chaque DAI dispose d'un support de valeur réelle.

Depuis 2019, avec le nouveau protocole MCD (*Multi-collateral DAI*), *MakerDAO* accepte d'autres tokens que l'Ether. Les valeurs de garantie sont variables, mais décidées par la gouvernance du protocole.

Margin Trading

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

Market Buy

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

MarketCap

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

Market Sell

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

Market Price

Le prix au marché (*market price*) est déterminé par la moyenne entre le *bid* le plus haut et l'*ask* le plus bas.

Masternode

C'est une machine connectée à un réseau. Dans le domaine de la cryptomonnaie, il s'agit d'un serveur dédié qui permet de faire transiter les communications propres aux transactions. Grâce aux règles de consensus, il améliore la sécurité de la blockchain. Il constitue alors une alternative au concept de preuve de travail (*Proof- of- Work*).

Afin de valider les transactions, le *Masternode* intègre différentes fonctionnalités dans son protocole. Selon les systèmes, il est ainsi possible de bénéficier d'un droit de vote sur un développement de projet ou une anonymisation des transferts de fonds. À ce titre, la vitesse de traitement est également optimisée. L'usage d'un *Masternode* peut donner lieu à une rémunération en contrepartie d'une contribution à l'amélioration et au développement du réseau.

Mème

Un mème est une image virale diffusée sur le web par le biais des réseaux sociaux, composée d'une photo explicite et d'un texte humoristique ou ironique, écrit, le plus souvent, dans une police large et blanche. Il s'agit de la francisation d'un mot anglais combinant les mots "gène" et "mimesis". Le terme se prononce /mi:m/ en anglais et /mɛm/ en français.

Le ton d'un mème est généralement humoristique, cynique ou ironique, et le message transmis souvent désabusé. Le mème existe sous de nombreuses formes, et possède l'avantage d'être rapide à lire et à comprendre, drôle, gratuit à mettre en place, et de marquer efficacement et durablement les esprits.

Parmi les mèmes les plus populaires de l'année 2020, citons le défi "LinkedIn, Facebook, Instagram, Tinder", également connu sous le nom de #DollyPartonChallenge. On peut également citer le grand classique "Sad Keanu", représentant l'acteur **Keanu Reeves** seul sur un banc, le Success Kid, cet enfant brandissant son poing sur la plage, le "Shut up and take my money" de **Futurama**.

Minage en Pool

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

Minage en Solo

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

Mineur

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

Mining / Minage

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

Minter

Procédé qui consiste à transformer (tokeniser) une œuvre d'art physique en un fichier numérique et l'émettre ensuite sous forme d'un jeton non fongible sur une blockchain. Le jeton une fois émis sur la blockchain, devient unique et identifiable.

Minting / Forgeage

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

Mobile wallet

C'est un portefeuille crypto qui, dans sa version mobile prend la forme d'une application à télécharger sur son smartphone. L'avantage premier de ce type de solutions réside dans la possibilité pour l'utilisateur de pouvoir accéder rapidement et facilement à sa cryptomonnaie et de pouvoir effectuer des achats physiques.

A ce stade, il existe deux options: une application qui va gérer le stockage en local (sur un smartphone, mais de la même manière que sur un ordinateur classique avec tous les risques que cela comporte en matière de sécurité: vol, piratage...) ou une application qui permettra d'accéder à sa cryptomonnaie, en se connectant à un serveur distant (ce qui présente les mêmes inconvénients, comme indiqué ci-dessus.

MP-Shield system

C'est un outil de protection contre la manipulation suspecte des prix (pump and dump) utilisé généralement par les plateformes de trading sur Marge.

Mt. Gox

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

Multisignal

Le concept *Multisignal* s'applique aux adresses multi-signatures en cryptomonnaie. Il peut également s'agir de comptes dédiés. Dans tous les cas, le principe repose sur un contrôle partagé des accès aux fonds. Le système fonctionne grâce à l'emploi d'une technologie de cryptographie spécialement conçue à cet effet.

On sollicite un dispositif *Multisignal* lorsqu'on doit obtenir une autorisation collective pour la validation d'une transaction. L'usage d'adresses multi-signatures permet d'améliorer la sécurité informatique liée au paiement et au stockage d'une cryptomonnaie. On recourt généralement à deux clefs numériques (une privée, et une seconde publique). Elles peuvent se présenter dans différents formats afin de produire une signature de type *Multisignal*.

N

Node / Nœud

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

NFT (Non Fungible Token)

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

Les NFTs étaient plutôt des tokens basiques associés à des images. Pour certains utilisateurs, cela représentait quelque chose d'unique à collectionner et pour d'autres cela ne valait rien puisqu'il suffisait juste de copier l'image pour l'avoir. Pour en acheter ou en vendre, il existe plusieurs plateformes spécialisées comme OpenSea¹⁴, Rarible¹⁵.

Depuis 2017, les NFT ont bien changé. Il est toujours possible d'acheter un *Cryptokitty* (le tout premier NFT lancé), mais aussi des œuvres d'art, des cartes de jeu, des noms de domaine ou même des tweets. Le patron de Twitter, **Jack Dorsey**, a mis aux enchères le 6 Mars 2021 son premier tweet.

¹⁴ https://opensea.io/

¹⁵ https://rarible.com/



Oracle

Dispositif qui permet d'intégrer des informations au sein d'une blockchain à partir de sources externes. Le principe fonctionne le plus souvent dans le cadre de contrats dits « intelligents ». Grâce à ces derniers, il est ainsi possible de lancer des applications de manière décentralisée, tout en respectant les protocoles techniques de sécurité.

Le contenu fourni par Oracle dépend des spécificités du contrat auquel il est associé. Ces sources d'information peuvent être issues du Web ou d'un objet non virtuel, comme une puce RFID ou même un capteur de mouvements. Le système se distingue par la fiabilité des données, ainsi que leur protection pour garantir leur intégrité. Il peut être utilisé sous une forme centralisée (un seul interlocuteur) ou décentralisée (plusieurs fournisseurs d'informations).

Order book (Carnet d'ordres)

Un *order book* ou carnet d'ordre en français est une liste électronique d'ordres d'achat et de vente d'un titre ou d'un autre instrument organisé par niveau de prix. Les carnets d'ordre sont utilisés par presque tous les échanges pour divers actifs tels que les actions, les obligations, les devises et même les cryptomonnaies.

Ces listes contribuent à améliorer la transparence du marché car elles fournissent des informations sur le prix, la disponibilité, la profondeur du commerce et qui initie les transactions. Sur l'interface de trading, le carnet d'ordre comporte trois parties : la liste des ordres d'achat (en couleur bleue), la liste des ordres de vente (en couleur rouge) et l'historique des ordres.

Open-source (la collaboration ouverte)

L'idée de base derrière le terme « open-source » fait référence aux scientifiques et aux chercheurs qui partagent librement et continuellement des informations, y compris des découvertes sur certains sujets. Le code source d'un logiciel en particulier est mis à la disposition des développeurs et des utilisateurs pour qu'ils puissent le modifier comme bon leur semble.

L'open-source est une approche du développement logiciel très pragmatique et axée sur les objectifs. Bitcoin et d'autres projets de cryptomonnaie se caractérisent par le fait qu'ils sont développés de manière transparente et collaborative par des entités indépendantes.

OTC (Over The Counter)

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

P

P2P (Peer-to-Peer) / Pair-à-Pair

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

Panic Buy

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

Panic Sell

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

Pool

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

PoS (Proof- of- Stake) / Preuve d'Enjeu

La preuve d'enjeu est une alternative au mécanisme de preuve de travail (Proof- of- Work) qui est critiqué pour son coût en électricité et son impact environnemental. L'algorithme de preuve d'enjeu tente de résoudre ces problèmes en supprimant entièrement le concept de minage et en le remplaçant par un mécanisme de *minage virtuel*.

La preuve d'enjeu demande à l'utilisateur de prouver qu'il possède une certaine quantité d'une cryptomonnaie donnée afin d'obtenir le droit de valider des blocs supplémentaires. L'algorithme va sélectionner aléatoirement un validateur parmi les personnes éligibles (plus une personne possède une grande quantité de la cryptomonnaie plus elle a de chances d'être sélectionnée) et va lui attribuer le droit de créer le prochain bloc. Tout comme dans le mécanisme de preuve de travail, la chaîne la plus longue est par défaut considérée comme la chaîne valide.

PoW (Proof of Work) / Preuve de Travail

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

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

Pré-minage

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

(Problème des) Généraux Byzantins

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

Pump

Hausse du prix d'une monnaie.

Pump and dump

Le "pump & dump", ou "pump and dump", est une technique de manipulation de marché qui s'apparente souvent, dans le monde des cryptomonnaies, à une escroquerie financière aux cours de bourses. Le pump and dump est souvent le fait d'acteurs importants présents sur un marché donné.

Le stratagème consiste à acheter d'énormes quantités d'une cryptomonnaie, afin d'en gonfler artificiellement le cours en espérant créer autour de cette bulle spéculative un sentiment de "Fomo".



Recovery phrase/Seed keyword

Recovery phrase (phrase de récupération en français), ou formule mnémonique, est un procédé qui permet à un détenteur de cryptomonnaies de les récupérer pour le cas où le support ou l'endroit où elles sont initialement stockées viendraient à faire défaut. Ainsi, il peut arriver que l'ordinateur sur lequel un propriétaire de cryptomonnaies a installé son wallet (avec ses bitcoins à l'intérieur) tombe en panne ou soit infecté par un virus. Dans cette hypothèse, il faut garder à l'esprit qu'à chaque fois que l'on installe un wallet, celui-ci fournit à son utilisateur une phrase, voire une formule, de récupération qui lui permettra, en cas d'incidents techniques, de récupérer ses fonds en utilisant cette formule mnémonique lors d'une nouvelle installation du wallet.

Partant de là, s'il y a un élément à protéger à tout prix et à tenir éloigner de tout acte malveillant, c'est bien cette phrase de récupération. La solution la plus simple reste de l'écrire sur une feuille de papier et/ou de la conserver précieusement au fond d'un coffre.

A contrario, il est fortement déconseillé de taper cette phrase sur n'importe quel site Internet, de la stocker sur un ordinateur, dans le *cloud*, sur une application de prise de note ou, pour des raisons évidentes de sécurité, sur des services de stockage en ligne de type *Google Drive* ou *Dropbox*. Tout juste pourra-t-on envisager de conserver le précieux sésame sur une clé USB dédiée à cet usage exclusif, tout en prenant soin d'en garder une copie physique séparée sur un simple morceau de papier.

Refill

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

Rekt (crypto) ou « Wrecked »

C'est une expression qui désigne une énorme perte. Issue au départ du monde du gaming, elle s'est propagée dans celui des cryptomonnaies où elle signifie une grosse perte d'argent sur un mauvais investissement. Parfois, cette expression se veut plus spécifique, lorsqu'un investisseur mise beaucoup sur une devise qui s'effondre peu de temps après, ou qui se fait arnaquer lors d'une « escroquerie de sortie ».

Se faire « *rekt* » est devenu fréquent pendant la bulle des cryptomonnaies de 2017 lorsque des investisseurs, qui étaient appâtés par l'envolée subite des valorisations, ont débarqué sur le marché des coins quelques semaines ou quelques mois avant l'effondrement des cours.

Sur les réseaux sociaux, le hashtag #rekt est utilisé par les investisseurs désabusés qui racontent leur malchance. Mais aussi par des trolls qui se moquent des mésaventures des investisseurs qui se sont montrés trop naïfs ou trop cupides, et donc jugés « responsables » de leur perte.

Rig de Minage

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

Ripple (XRP)

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

ROI (Return on Investment)

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

Royalties

Droit d'auteur, redevance due au propriétaire d'un brevet ou d'une marque ou encore au propriétaire du sol sur lequel sont assurées certaines exploitations. Dans le domaine de la technologie blockchain, cela représente un pourcentage défini au préalable, que le créateur d'un Token non Fongible (NFT) touche à chaque fois que son œuvre est revendue.

S

Satoshi

Un Satoshi représente la plus petite unité du Bitcoin (1 Satoshi = 0.00000001 BTC). C'est une unité souvent utilisée dans le milieu du trading. Elle fait référence au créateur du bitcoin : **Satoshi Nakamoto**.

Satoshi Nakamoto

Satoshi Nakamoto est le pseudonyme de la personne ou du groupe de personnes qui, de 2009 à 2010, ont conçu et créé Bitcoin. C'est aussi le fondateur de *bitcoin.org* et du forum *bitcointalk*.

Scalabilité

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

Scalping

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

Scam / Arnaque

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

Security token

Le security token définit un titre ou actif numérique. Respectant le test de Howey, le security token est considéré comme un véritable investissement ou pur actif financier avec, pour son détenteur, des objectifs de profits à plus ou moins long terme. Dit autrement, le security token représente l'équivalent numérique d'une prise de parts de capital dans une entreprise, une part de propriété dans l'achat d'un appartement mis en location, etc.

Segwit (Segregated Witness)

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

Sell wall (crypto)

En cryptomonnaie, le « wall » désigne un ordre ou un ensemble d'ordres similaires qui représente un volume important de transactions et prenant l'allure d'un mur sur le carnet d'ordres d'une plateforme d'échanges. On parle de « sell wall » quand une vente importante a lieu ou bien quand de nombreux ordres de vente au même prix ont été passés simultanément pour la même devise.

SHA-256

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

Sharding

Technique avancée de gestion de base de données connue en Informatique, le *sharding* peut être également utilisé dans le domaine de la cryptomonnaie. De manière générale, en Informatique, le *sharding* permet une architecture de données qui est parfois nécessaire. En effet, lorsque l'on fait face à un très grand volume de données (*Big Data*), il est préférable, pour les traiter plus rapidement, de les séparer en plusieurs jeux de données (*Data Set*).

Développée par Ethereum pour être appliquée à la cryptomonnaie, la technique du *sharding* sert dans ce cas à partitionner les données de la blockchain (notamment tout l'historique des échanges réalisés entre ses utilisateurs depuis sa création), et à ne pas concentrer sur les blocs d'une seule blockchain le processus de validation de chaque nouvelle transaction. Avec le *sharding*, il est possible de réaliser un plus grand nombre de transactions en même temps, car la base de données est partagée en plusieurs sous-parties autonomes.

Share

Morceau, part, qu'un mineur aura mérité selon la contribution qu'il aura fourni à sa pool de minage.

Shitcoin

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

Short

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

Sidechain

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

Silk Road

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

Slippage (Dérapage)

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

Smart Contract / Contrat Intelligent

Le concept de *smart contract* fut établi au milieu des années 1990 par **Nick Szabo**, scientifique et cryptographe. Un smart contract est l'équivalent informatique d'un contrat traditionnel.

Cependant, à la différence d'un contrat traditionnel, dont l'exécution est régie par un cadre juridique, celle du smart contract ne nécessite l'intervention d'aucun tiers de confiance et est, en tant que protocole informatique, régie par le code informatique.

Un smart contract est un logiciel qui ne dispose en tant que tel d'aucune autorité juridique. Le smart contract s'appuie sur la technologie blockchain pour sécuriser et rendre infalsifiables les termes et les conditions de son exécution.

En pratique, un smart contract exécute automatiquement des conditions définies au préalable et inscrites dans une blockchain. Seul le code informatique décide de l'exécution totale ou partielle d'un contrat. La sécurité d'un smart contract est-elle pour autant absolue ? Non, car a minima des failles de sécurité dans le code open source pourraient, en certaines circonstances exceptionnelles, être exploitées pour modifier les termes d'un contrat.

Moins coûteux, plus rapide et ne nécessitant aucun tiers de confiance, le smart contract trouve déjà de multiples applications dans les domaines de l'assurance, de l'immobilier ou de la "supply chain", pour ne prendre que quelques exemples. Le terme anglais "smart contract" signifie littéralement "contrat intelligent".

Smart grids

C'est la dénomination générale applicable à l'ensemble des technologies et des infrastructures "intelligentes" installées. Les smart grids sont un vecteur de flexibilité, car ils permettent de gérer plus finement l'équilibre entre production et consommation. Ils se caractérisent également par leur fiabilité, en améliorant notamment l'efficacité et la sécurité des réseaux, par leur accessibilité, en favorisant l'intégration des sources d'énergies renouvelables sur l'ensemble d'un réseau donné, et par le fait qu'ils permettent de réaliser des économies en apportant, grâce à une meilleure gestion du système, des économies d'énergie et une diminution des coûts (à la production comme à la consommation).

Concernant plus spécifiquement l'électricité, le "smart grid", est un dispositif de réseaux d'électricité, basé sur des technologies informatiques qui, en collectant et en analysant des informations sur l'état d'un réseau électrique, contribue à ajuster les flux d'électricité entre producteurs, distributeurs et consommateurs. On peut traduire le terme de "smart grids" par celui de "réseaux électriques intelligents".

Soft Fork

Modification mineure de la chaîne de blocs sans séparation en deux parties (split). Par exemple, le *segwit* est implémenté via un soft fork.

Software wallet

Un software wallet, que l'on peut traduire par portefeuille logiciel, est un programme logiciel destiné à stocker une ou plusieurs cryptomonnaies. Le software wallet se présente sous trois

formes: sur un ordinateur, en version mobile ou en ligne. La première solution, dénommée desktop wallet, est un logiciel qui va permettre de stocker une cryptomonnaie directement sur un ordinateur de bureau ou sur un ordinateur portable. L'utilisateur de ce type de softwares wallets, qui est aussi le détenteur des cryptomonnaies stockées, a, ici, la main sur ses devises. Ce faisant, c'est également à lui qu'il appartient d'en sécuriser le stockage, ce qui n'est pas toujours chose aisée pour un utilisateur lambda.

Solidity

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

Spread

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

Stable coin

Token dont la valeur est indexée sur une valeur de référence (le dollar, l'euro,...) afin de conserver une certaine stabilité.

Stack

Désigne l'ensemble du capital en cryptomonnaies possédé par un investisseur.

Staking

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

STO (Securities Token Offering)

Procédé qui consiste en l'émission de parts de capital d'une entreprise sous la forme de « tokens » sur une blockchain.

Stop Loss

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

Support

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

T

Take Profit

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

Testnet

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

To the moon

Il s'agit d'un mème. Lorsqu'on croit à une cryptomonnaie ou lorsqu'un pump a lieu, on dit de celle-ci qu'elle atteindra la lune : to the moon.

Tokenisation

Procédé qui vise à représenter un actif, numérique ou physique, par un « token » sur une blockchain, lui faisant ainsi bénéficier de ses caractéristiques (liquidité, cessibilité, divisibilité etc.).

Tokenomics

Terme utilisé actuellement pour désigner plusieurs choses dans l'économie virtuelle. Premièrement, la *Tokenomics* peut définir au sens large la science étudiant le fonctionnement des cryptomonnaies, de leur création à leur suppression, en passant par leur gestion et leurs mécanismes de fonctionnement (notamment le fonctionnement des blockchains). Ce mot de *Tokenomics* est également parfois utilisé pour désigner plus particulièrement l'écosystème économique d'un jeton (ou token) créé par une blockchain, à savoir l'utilité du jeton, la quantité de jetons à émettre, etc. Enfin, *Tokenomics* peut aussi désigner parfois le processus de création d'un système économique basé sur les cryptomonnaies, et qui viendrait petit à petit se substituer au système économique traditionnel, grâce au soutien d'une communauté grandissante.

Tokens / Jetons

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

Token de gouvernance

C'est un token émis par une plateforme, comme l'YFI de Yearn Finance. Il permet de prendre toutes les décisions au sein du protocole.

Top / Sommet

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

TOR (The Onion Router) / Le Routage en Oignon

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

Trading Bot

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

Trailing stop (Stop suiveur):

C'est un ordre utilisé en Trading, qui se déclenche en fonction d'une variation du prix fixée par le *trader* (le sentier), mais évolue avec le prix du marché. Dans le cas d'un achat, si le prix du marché baisse, le seuil de déclenchement du stop suiveur baisse également. Par exemple, si vous placez un ordre d'achat stop suiveur à 41000\$ avec un sentier de 1000\$, l'ordre se déclenche lorsque le prix atteint 42000\$. Mais si le marché baisse, par exemple à 40500\$, le nouveau seuil de déclenchement sera alors placé à 41500\$.

Turing-complet

L'expression "Turing-complet" fait référence au mathématicien et cryptologue anglais **Alan Turing,** un des précurseurs de l'informatique, qui décrivit un modèle pour définir les concepts d'algorithme, de programmation et de décidabilité donnant naissance à la fameuse machine de Turing. C'était une sorte d'ordinateur avant l'heure, pouvant déchiffrer les messages codés des Allemands durant la seconde guerre mondiale.

Un langage de programmation est dit "Turing-complet" s'il peut permettre de simuler une machine de Turing, avec le même pouvoir expressif et la même calculabilité. En particulier, un langage Turing-complet doit permettre d'exécuter des **fonctions récursives** ou "calculables", nécessaires pour mettre en place des **boucles conditionnelles** (if, then, else) et plus généralement pour que le langage soit **déterministe** (les mêmes fonctions appliquées aux mêmes arguments donneront toujours le même résultat).

Le langage de programmation "solidity" est un langage "Turing-complet", contrairement à "script" de Bitcoin, qui ne permet que de programmer des transactions financières conditionnelles avec son jeu d'opcodes.

TXID (ID de transaction bitcoin)

Dans la blockchain, l'empreinte (hash) d'une transaction bitcoin est son identifiant. A chaque transaction bitcoin est rattachée une empreinte cryptographique, que l'on appelle identifiant de transaction (TXID).

U

Utility token

C'est un « jeton utilitaire » dont la principale fonction consiste à permettre l'accès futur à un service ou à un produit proposé par une entreprise. Lorsque vous investissez dans des *utility tokens*, votre objectif final est de pouvoir vous offrir ou utiliser un service spécifique.

À l'inverse d'un security token, un utility token ne peut pas véritablement être considéré comme un actif. Pour autant, l'utility token peut faire l'objet de spéculations. Si le service auquel il est associé voit sa popularité augmenter, la valeur de l'utility token est susceptible d'évoluer à la hausse. Parmi les plus prometteuses, il est possible de citer **Storj** (location de stockage sur le Cloud), **iExec** (location de puissance de calcul), **Civic** (protection de l'identité), **Augur** (prédiction d'événements), **BAT** (moyen de paiement entre producteurs et utilisateurs de contenus des navigateurs) ou encore **Snapparazzi** (une sorte de nouveau YouTube)



Vanity Address

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

Vault

Coffre-fort dans lequel les utilisateurs déposent leurs cryptomonnaies. Le *vault* fournit et verrouille de la liquidité dans un protocole pour obtenir des récompenses. Quand l'utilisateur sort du *vault*, il récupère ses cryptomonnaies et une partie des récompenses obtenues par le vault. Pour résumer, le vault permet à l'utilisateur de déléguer son *Yield Farming* au lieu de le gérer lui-même. Le *vault* est une « prestation de service » de *Yield Farming*.

Vitalik Buterin

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

Volatilité

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



Wall / Mur

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

Wallet / Portefeuille

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

Wallet determinist

Le wallet determinist, ou HD wallet (pour "hierarchical deterministic wallet"), est une solution qui, dans le cadre de l'adoption de la cryptographie asymétrique (clé publique / clé privée), permet au détenteur de cryptomonnaies de générer de nombreuses clés privées à partir d'un seul point de départ appelée graine (ou "seed" en anglais).

En pratique, cette graine initiale, que l'utilisateur devra impérativement sauvegarder en toute sécurité (de préférence en "cold storage", c'est-à-dire sur un support non connecté à Internet pour ne pas tenter les cybercriminels), est une valeur aléatoire (de 128, 156 ou 512 bits) qui peut se présenter sous la forme d'une douzaine de mots en anglais.

A partir de cette graine initiale, il sera possible de créer de nombreuses clés privées dérivantes les unes des autres. Facile d'utilisation, le HD wallet permet au détenteur de cryptomonnaies, après avoir préalablement sauvegardé la graine initiale, de régénérer à partir d'elle et à tout moment l'intégralité de son portefeuille.

Wash trading

Le "wash trading" est une escroquerie, une forme de manipulation du marché qui consiste à vendre et à acheter la même devise simultanément. Le but de la manœuvre est de donner l'illusion d'une demande imaginaire pour une cryptomonnaie, en boostant de façon artificielle le volume des transactions. Ici, les cibles sont les investisseurs qui vont prendre position sur une

devise en croyant deviner un engouement, qui est en réalité faux. Lorsque le cours a suffisamment monté, l'orchestre de l'escroquerie revend ses coins pour empocher une plus-value au détriment des autres acheteurs, qui eux perdent leur mise.

Le *wash trading* n'est pas un terme propre à l'univers des cryptomonnaies mais à celui de l'investissement, en général. Il désigne une forme d'escroquerie.

Weak Hands

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

Whale / Baleine

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

Whitepaper / Livre Blanc

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



Yield Farming

Le *Yield farming*, littéralement « l'agriculture de rendement », est une approche qui utilise plusieurs stratégies pour optimiser les rendements générés par les cryptomonnaies. Il s'agit d'un processus dans lequel les utilisateurs fournissent des liquidités aux protocoles DeFi, et sont récompensés par un rendement, sous forme de tokens (jetons).

Le phénomène de Yield farming s'explique par l'intérêt croissant pour la DeFi, et l'arrivée massive de liquidités sur des marchés monétaires tels que Compund. L'idée de départ du protocole était très simple : mettre en relations prêteurs et emprunteurs. Les plateformes utilisent un système de pool de liquidités permettant aux prêteurs de fournir des actifs au marché, et aux utilisateurs d'emprunter sur ce marché.

En plus du taux d'intérêt et de la commission perçue à chaque transaction, les fournisseurs de liquidités sont rémunérés en jetons. Les tokens sont valorisés par le marché, et peuvent être vendus ou conservés. Les rendements sont si importants qu'ils incitent les utilisateurs à fournir des liquidités afin d'amorcer les ressources financières d'un nouveau protocole de finance décentralisée.

C'est cette double récompense qui a donné naissance au terme de Yield farming. La tendance de Yield farming s'est ensuite démocratisée avec la création de nouveaux protocoles DeFi et l'évolution des stratégies. Désormais, les utilisateurs tentent de tirer parti de l'imbrication des différentes applications de la DeFi, avec comme objectif le cumul des récompenses.

RESSOURCES UTILES

RESEAUX SOCIAUX

Chaînes YouTube

Quest4Profit; le Journal du Coin; Hasheur (Owen Simonin); Cryptoast; Crok; Benjamin Cowen; CryptoMatrix; Bitcoin for Beginners; Cryptonews; Jeanjean la bricole; Crypto Flash France; MoneyRadar; Positive Internet Solution
Les canaux Telegram spécialisés

Tweeter

SITES WEB

Site de référence pour le listing des cryptomonnaies par leurs prix et par capitalisation du marché :

coinmarketcap.com; coin360.com; curvemarketcap.com; coingecko.com; coinbase.com; Binance.com

Site de référence pour les actualités crypto:

ftx.com; theblockcryptp.com; coindesk.com; github.com; cointelegraph.com; positiveinternetsolution.com; decrypt.co; cryptoslate.com; journalducoin.com; Cryptoast.fr; actufinance.fr; crypto-monnaie.pro; coindesk.com; cex.io

Sites de références pour le listing des projets DeFi :

defipulse.com; defimarketcap.io; defillama.com

Sites de référence pour le listing et des informations sur des projets NFT :

Cryptoslam.io; playtoearn.net; playtoearn.online; rarity.tools; DappRadar.com; tweeter.com; discord.com

Sites de référence pour des informations sur le Metaverse, la blockchain et le minage :

facebook.com; oculus.com; exclusible.com; coinmarketcap.com; decentraland.org; just-mining.com

Sites de référence pour trouver les meilleures formations aux cryptomonnaies et à la blockchain :

Positiveinternetsolution.com; alyra.fr; kryptosphere.org; cryptoast.fr; journalducoin.com

Sites de référence pour trouver des emplois aux métiers de la blockchain et aux cryptomonnaies, ou en publier :

onchainJobs.io; cryptocurrencyjobs.co

Site de référence pour trouver les gas fees en temps réel et où faire des opérations crypto au meilleur frais :

Gasnow.org; etherscan.io; l2fees.info; ultrasound.money; bitpand.com; paraswap.io

Site de référence pour comparer les cryptomonnaies, les projets DeFi et les projets NFT entre eux et par rapport aux autres marchés d'actifs :

compagniesmarketcap.com; marketcapof.com

Les meilleurs Marketplace des NFTs :

Opensea.io; rarible.com; fractional.art; superrare.com; atomicasset.io; foundation.app; knoworigin.io; async.art; nft-catalog.com; nftroyaltoken.com

GAGNEZ DU TEMPS ET DE L'ARGENT AVEC CRYPTO FORTUNE TOME 2



CRYPTO FORTUNE Tome 2

Théorie et Pratique, un guide complet pour débutants et professionnels sur le marché des cryptomonnaies

Mettez rapidement la main sur un raccourci qui vous guide à travers tout l'écosystème de la blockchain et des cryptomonnaies sans que vous n'ayez plus à beaucoup réfléchir!

CRYPTO FORTUNE Tome 2 est un ouvrage qui contient toute la pédagogie, l'information et les outils pratiques, et qui vous permet de les mettre rapidement en pratique afin de s'enrichir sur le marché des cryptomonnaies.

La bonne nouvelle, c'est que pour s'enrichir sur le marché des cryptomonnaies, il n'est pas nécessaire d'avoir le QI de Vitalik Buterin. Vous n'avez pas non plus besoin d'avoir la fortune de Satoshi Nakamoto. Ce dont vous avez besoin, c'est d'étudier tout simplement le sujet.

Qu'allez-vous apprendre dans ce Livre?

226 pages réparties en 3 sections qui sont :

Section 1 : La théorie

Tout ce que vous devez savoir sur le Bitcoin, les autres cryptomonnaies, la technologie *blockchain*, les *Smart contracts*, le marché des cryptomonnaies et tous ses composants à savoir les plateformes d'échange, les portefeuilles en cryptomonnaies, le minage, les ICO, les NFTs et la DeFi.

Section 2: Pratique

Je vous livre étape par étape, des outils pratiques (avec des exemples concrets) et des conseils à mettre rapidement en œuvre pour être rentable en fonction de votre profil d'acteur sur le marché.

Vous êtes débutants ou professionnels en crypto-investissement, crypto-trading, crypto-mining, ou vous désirez créer votre propre cryptomonnaie, parfait. Vous souhaitez

également connaitre le régime fiscal qui s'applique aux plus-values des gains sur les cryptoactifs dans votre pays, normal.

Trouvez ici dans cette section, 8 chapitres dont chacun vous livre les nouveaux outils prêts sur le marché qui vont faire de vous non seulement des cryptos investisseurs, traders ou mineurs, mais aussi des créateurs de cryptomonnaies. Vous découvrirez également comment encaisser de façon automatique, les paiements en crypto dans votre commerce.

Section 3 : Opportunité d'Affaires

Découvrez ce modèle d'économie inclusive qui, en plus de vous permettre d'avoir accès à des formations qualifiées et sponsorisées dans divers domaines en lien avec l'Informatique, vous livre des astuces simples à utiliser pour gagner 2000€/mois de revenus supplémentaires sans avoir investi un seul centime d'euro dans les cryptomonnaies.

NB:

En décidant aujourd'hui d'apprendre vous-même à investir sur le marché des cryptos, sachez bien que vous contribuez ainsi à la réalisation du rêve de la dénationalisation de la monnaie, à l'adhésion massive à un système pair à pair sans tiers de confiance et sans autorité centrale qui permet de transférer de la valeur à l'échelle mondiale! **CHANGER LA MONNAIE, C'EST CHANGER LE MONDE.**

À qui s'adresse ce livre?

CRYPTO FORTUNE Tome 2 ne vous promet pas que vous alliez être millionnaire en 28 jours.

Honnêtement, il n'y a pas de formule magique.

« Le succès sur le marché des cryptomonnaies est le fruit de plusieurs années de persévérance, de recherche minutieuse, de décisions rationnelles, d'approches réalistes et d'investissement en temps et en patience ».

Il n'est pas non plus destiné aux investisseurs chasseurs de trésors qui espèrent faire ×5000 sur des cryptomonnaies obscures conseillées par des pseudos spécialistes de YouTube.

Andreas Antonopoulos nous rappelle que : « *Bitcoin n'est pas conçu pour rendre ses utilisateurs riches* [même s'il engendre des millionnaires]. *Il est conçu pour rendre ses utilisateurs libres* ».

Par contre, CRYPTO FORTUNE s'adresse :

à ceux qui veulent se former avant de se lancer sur le marché des cryptomonnaies,

- à ceux qui veulent investir et bâtir un empire financier pour leur avenir,
- aux investisseurs déçus qui veulent repartir sur de bonnes bases : avoir des stratégies, posséder une vision du marché à moyen et long terme, posséder toutes les connaissances nécessaires pour ne plus reproduire les mêmes erreurs,
- aux investisseurs qui veulent savoir comment être en règle avec la fiscalité des crypto-actifs dans leur pays de résidence,
- aux investisseurs qui veulent être autonomes dans leur prise de décision,
- à ceux qui veulent se lancer dans le trading crypto, dans le minage ou dans la création de leurs propres monnaies numériques, ou encore développer une compétence aux métiers de la blockchain, mais ne savent pas par où commencer.

Comment se procurer ce livre?

CRYPTO FORTUNE Tome 2 est disponible en vente sur mon site internet www.positiveinternetsolution.com au format papier et en Ebook, et avec une garantie 100% satisfait ou remboursé de 14 jours.

OPORTUNITE D'AFFAIRES

MA STRATEGIE POUR VOUS FAIRE GAGNER 2000€/MOIS SANS AVOIR INVESTI UN SEUL CENTIME D'EURO DANS LES CRYPTOMONNAIES.

Vous êtes sur le point de découvrir un business modèle qui, en plus de vous permettre d'avoir accès à des formations qualifiées et sponsorisées dans divers domaines, vous livre des astuces simples à utiliser pour gagner jusqu'à 2000€/mois de revenus supplémentaires sans avoir investi dans les cryptomonnaies.

POSITIVE INTERNET SOLUTION¹⁶ est une société informatique créée le 30 novembre 2018 au Togo par Kodjo Helle et André Segla.

Ce que nous faisons :

Nous accompagnons tous les internautes qui ont la rage de gagner plus d'argent en ligne afin d'assurer leur indépendance financière. Pour se faire :

- 1-Nous aidons tous les internautes à gagner jusqu'à 2000€ par jour à l'aide de notre business model basé sur l'affiliation.
- 2- Nous sponsorisons des formations (jusqu'à 40% des frais) aux métiers de la blockchain, au Marketing digital, à L'IA, au Développement web et d'application mobile pour tous nos affiliés qui souhaitent se former auprès des formateurs dont la réputation en matière de formation n'est plus à prouver.

Comment nous travaillons:

- 1- Nous disposons d'un Marketplace d'E-learning (POSITIVE ACADEMY) qui héberge toutes nos formations. La vision de POSITIVE ACADEMY est d'être le seul lieu de regroupement de toutes les meilleures formations en lien avec l'internet. Principalement celles de nos formateurs africains de la diaspora et sur le continent.
- 2- des collaborations avec des entrepreneurs et formateurs à succès dans des partages d'opportunités d'affaires en lignes dans notre forum POSITIVE BUSINESS.

¹⁶ https://www.positiveinternetsolution.com/

- 3- Un programme de récompense pour la publication des articles et actualités en lien avec le secteur de l'informatique. Principalement le secteur de la blockchain et du web3.0
- 4- Un média qui publie des actu crypto, Blockchain, Web3.0, Finance, la bourse.
- 5- Une fondation "Crypto-leader" qui accompagne tous les apprenants formés aux métiers de la blockchain dans le développement des projets à plus forte valeur ajoutée de ces derniers. Laquelle fondation est en phase de planification et comporte un volet de création et promotion des NFTs.
- 6- Une librairie et une maison d'édition en ligne (Les Éditions CRYPTO FORTUNE) pour la publication et la vente de vos ouvrages au format PDF et papiers.

POSITIVE ACADEMY



<u>Une super académie qui permettrait à chaque Infopreneur, Coach, Consultant et Formateur de gagner plus de clients en ligne sans faire de publicité, n'existe pas encore dans l'univers du web francophone.</u>

<u>Une super académie dans laquelle tout étudiant à la quête d'une formation de haute qualité</u> ne se demanderait plus où trouver de l'argent pour financer ses formations, n'existe pas encore dans l'univers du web francophone.

Jusqu'au 02 mars 2022, date à laquelle **POSITIVE ACADEMY** a ouvert ses portes.

Imaginez ce que serait votre vie si <u>chaque année 10.000 internautes à travers le monde</u> vous donnent seulement chacun 40€ supplémentaires sans que vous n'ayez besoin de <u>frapper à leurs portes avec des coûts publicitaires suicidaires.</u> 10.000x40€ = 400.000€ chaque année que vous gagnez depuis le confort de votre demeure. Et si c'est 20.000, 30.000 ou 40.000 internautes ? Faîtes vous-même les calculs.

Comment ça marche concrètement?

Pour les apprenants, vous payez 50€ chaque année et cela vous donne accès au programme d'affiliation avec ses trois (03) avantages majeurs à savoir :

- Vous obtenez un code d'affiliation qui vous permet de gagner 50% à 80% de commission sur l'inscription de vos filleuls.
- Vous bénéficiez des formations sponsorisées par POSITIVE ACADEMY en obtenant des réductions de 10% à 40% sur les frais de vos formations chaque année.
- Vous gagnez gratuitement mon Ebook CRYPTO FORTUNE Tome 2 (valeur 11,5€)

Notre programme d'affiliation est élaboré dans le but de résoudre le principal problème à l'accès des formations qualifiées en Afrique, qui est le coût des formations. Avec notre programme d'affiliation, l'apprenant ne se pose plus de question au sujet de l'argent dont il a besoin pour financer ses formations. Car les avantages que lui offrent l'affiliation, l'aident à gagner ses frais de formation au sein de notre académie. Ce que ne permettent pas les autres structures qui offrent des formations en ligne.

<u>Pour les apprenants</u>, <u>les commissions de parrainage sont réparties en deux (02) niveaux de qualification à savoir :</u>

- De 01 à 10 affiliés vous gagnez 50%, soit 25€ par affiliation.
- De 11 et plus vous gagnez 80%, soit 40€ par affiliation.



PROGRAMME D'AFFILAION DE POSITIVE ACADEMY POUR LES APPRENANTS Tableau des gains de parrainage en fonction du nombre d'affiliés.

Affiliés	[01 ; 10]	[10;+∞[
TAUX	50%	80%	
Montant	50%X50€	80%X50€	
par parrainage	= 25€	= 40€	
TOTAL	10X25€	+∞	
	= 250€		

<u>Comment sont sponsorisées les formations pour les apprenants inscrits au programme</u> d'affiliation ?

- De 10 à 20 affiliés vous bénéficiez de 10% de réduction sur les frais de formation.
- De 20 à 50 affiliés vous bénéficiez de 20% de réduction sur les frais de formation.
- De 50 à 100 affiliés vous bénéficiez de 30% de réduction sur les frais de formation.
- De 100 affiliés et plus vous bénéficiez de 40% de réduction sur les frais de formation



PROGRAMME D'AFFILAION DE POSITIVE ACADEMY POUR LES APPRENANTS Sponsoring des formations en fonction du nombre d'affiliés.

Affiliés	[10;20]	[20;50]	[50 ; 100]	[100;+∞[
TAUX DE	10%	20%	30%	40%
SPONSORING				

Pour les formateurs dont les modules de formation sont acceptés par POSITIVE ACADEMY, vous ne payez pas les 50€ la première année. Vous commencez le paiement à partir de la seconde année et cela vous donne accès au programme d'affiliation.

<u>Pour les formateurs, les commissions de parrainage sont réparties en quatre (04) niveaux de qualification à savoir :</u>

- De 01 à 10 affiliés vous gagnez 20%. C'est à dire 20%X50€ = 10€ pour chaque personne qui s'inscrit dans le programme d'affiliation via votre code d'affiliation.
- De 11 à 20 affiliés vous gagnez 30%, soit 15€ par affiliation.
- De 21 à 50 affiliés vous gagnez 50%, soit 25€ par affiliation
- De 51 et plus vous gagnez 80%, soit 40€ par affiliation



PROGRAMME D'AFFILAION DE POSITIVE ACADEMY POUR LES FORMATEURS Tableau des gains de parrainage en fonction du nombre d'affiliés.

Affiliés	[01;10]	[10;20]	[20;50]	[50 ; + ∞[
TAUX	20%	30%	50%	80%
Montant	20%X50€	30%X50€	50%X50€	80%X50€
par parrainage	= 10€	= 15€	= 25€	= 40€
TOTAL	10X10€	10X15€	30X25€	+∞
	= 100€	= 150€	= 750€	

NB:

- Un formateur dont les modules de formation ne sont pas acceptés par POSITIVE ACADEMY est traité au même titre qu'un apprenant.
- Le programme d'affiliation a une durée de validité de 365 jours. Chaque année, Apprenants et formateurs doivent renouveler leur inscription en payant les 50€ avant expiration. Celui qui ne le fait pas, perd toutes les commissions à gagner sur ses affiliés ayant renouvelés leur inscription.

POSITIVE ACADEMY se veut être le lieu du rassemblement de plusieurs formations liées au secteur informatique dont les formations aux métiers de la blockchain, au Marketing digital, à l'IA, au Développement de site web et d'application mobile.

Si vous êtes Infopreneur, Coach, Consultant et Formateur avec une bonne réputation en matière de formation en ligne, alors voici comment nous envisageons cette collaboration :

- Nous offrons un espace formateur sur notre plateforme sans aucun frais à payer.
 Le formateur y poste les informations sur ses offres de formations exactement comme sur son site officiel.
- POSITIVE ACADEMY organise des campagnes publicitaires afin de pouvoir recruter des apprenants.
- POSITIVE ACADEMY encaisse les paiements et les renvoie par la suite au formateur par virement bancaire.
- Le formateur fait découvrir notre programme d'affiliation à sa communauté qui serait infiniment heureuse de la découverte.
- Le formateur s'engage à ne pas développer notre programme d'affiliation ailleurs sur le web.
- POSITIVE ACADEMY s'engage à ne pas accueillir d'autres structures offrant les mêmes formations du formateur avec qui elle collabore.

Comment se déroulent les formations?

Des vidéos, des guides digitaux au format que vous désirez pour passer à la pratique, ainsi que des coachings en live. Tout cela dans un espace privé du formateur, et entièrement sécurisé.

Pourquoi nous faire confiance?

POSITIVE INTERNET SOLUTION est une société immatriculée au registre du commerce et des sociétés de Lomé sous le numéro TG-LOM 2018 A 7130. Siège social : Rue Malfakassa, Qt Kagnikopé, Lomé. Le site internet positiveinternetsolution.com est édité et diffusé par la société POSITIVE INTERNET SOLUTION. Notre équipe collabore avec les meilleurs acteurs dont la réputation dans l'espace francophone n'est plus à prouver.

Voici le lien pour vous inscrire : https://www.positiveinternetsolution.com/register

Prenez soin de copier et coller le code d'affiliation de votre parrain dans la case correspondante

BONUS SPECIAL POUR LES MEMBRES DU PROGRAMME D'AFFILIATION

Vous obtenez votre accès GRATUIT à l'espace privé du Forum POSITIVE BUSINESS PRO.

POSITIVE BUSINESS PRO est le pôle investissement de POSITIVE INTERNET SOLUTION.

Sur le web et sur le marché des cryptomonnaies en particulier, le défi est de taille. Il implique de faire converger des paramètres nombreux et parfois antagonistes : état du marché et du cours de ses principales devises numériques bien sûr, solidité des acteurs auxquels on accordera sa confiance, surface financière disponible et jusqu'à sa propre capacité à gérer le risque, et tolérer l'aléatoire.

Pour atteindre ces objectifs ambitieux, quelques règles universelles s'appliquent. Bien connaître le périmètre et faire partie des bons réseaux en font partie. Se regrouper afin de mettre en commun les compétences et capacités de chacun, tout en diluant le risque en est une autre. Cette alchimie s'épanouit tout particulièrement dans le cadre d'un club privé d'investisseurs, ainsi que le propose le « FORUM POSITIVE BUSINESS PRO ».

Dans le forum :

- Vous pouvez partager vos opportunités d'affaires ou vos offres de formations qui ne sont pas listés à POSITIVE ACADEMY,
- Vous pouvez vendre vos livres et services et garder tout le bénéfice pour vous seul,
- Nous sélectionnons les produits et services à plus forte valeurs ajoutées que nous mettons en vente sur notre site web positiveinternetsolution.com pour vous sans aucun frais payé et vous gardez tous le bénéfice pour vous seul,
- Des invités surprise. Vous avez en live chaque moi, un web entrepreneur à succès qui vient vous édifier sur les nouveaux outils marketing et technologiques qu'il utilise pour être ultra rentable et comment vous pouvez vous aussi vous en inspirer.

NB:

Malgré un accès gratuit au forum POSITIVE BUSINESS PRO, vous n'êtes pas libre de faire ce que bon vous semble. **Vous devez tenir compte des deux points suivants** pour vous garantir de façon pérenne un accès illimité:

Point N°1: Etiquette du FORUM POSITIVE BUSINESS PRO

- POSITIVE BUSINESS est un forum entièrement économique, éducatif et à but lucratif. C'est- à- dire qu'il permet de se former au webmarketing, à la blockchain, à l'IA, et plus, de vendre et d'acheter les biens et services sur internet.
- Il est ouvert à tous sans distinction de race, de nationalité, de sexe, d'appartenance religieuse ou politique à condition d'avoir 18 ans d'âge.
- Vous n'êtes ni supérieur, ni inférieur aux autres membres. Chacun collabore avec les autres, dans un respect mutuel.
- Il n'y a pas d'argent facile. Ici, vous serez en compagnie des entrepreneurs qui sont prêts à gratter ensemble pour aller chercher les centimes d'euro partout sur le web. Si c'est les gains faciles que vous recherchez, alors vous pouvez passer votre chemin.
- Il n'est pas un groupe anonyme. Chacun peut donc s'identifier donc avec sa vraie identité, ou non.
- Il garantit la protection de votre vie privée et de vos informations personnelles.

• Il adhère aux valeurs partagées par les promoteurs de la technologie blockchain et des cryptomonnaies : dénationalisation de la monnaie, désintermédiation et décentralisation dans les transactions de valeurs entre individus.

Point N°2 : Règlement intérieur du FORUM POSITIVE BUSINESS PRO Vous serez immédiatement exclu du forum si :

- Vous faites la promotion d'une idéologie politique ou religieuse, des sites pornographiques ou de groupes terroristes.
- Vous publiez les offres de produits ou services illicites (stupéfiants, médicaments contrefaits, trafic d'êtres humains, d'armes,....)
- Vous faites la promotion d'une crypto obscure, d'une opportunité louche qui promet de rendre des gens millionnaires en 28 Jours. Nous n'autorisons pas les inventeurs de "Poyais".
- Vous tenez des propos racistes, vous publiez des images ou vidéos qui incitent à la violence.
- Vous répandez des rumeurs, des informations fausses ou non fondées.
- Vous lancez des débats improductifs, un spam, des liens vers d'autres groupes.
- Vous partagez des annonces et publicités personnelles sans notre consentement.

Toute publication d'offres de formations, de produits ou de services, doit être étudiée en amont avec l'équipe dirigeante du Forum.

Conclusion

Le milliardaire américain **Paul Tudor Jones** affirme je cite : « *Investir dans les cryptomonnaies c'est comme investir avec Steve Jobs et Apple ou investir dans Google à ses débuts* ». À POSITIVE INTERNET SOLUTION, nous avons la conviction que la blockchain, c'est l'avenir de la finance mondiale et notre idée, c'est de rendre accessible cet univers à un plus grand nombre. C'est pourquoi nous ne sommes pas là pour vite faire du fric et se barrer. D'ailleurs, **Pourquoi passer sa vie à fuir les autorités quand on peut devenir riche rapidement et légalement ?** Nous avons un projet décent qui cherchera à créer ou apporter quelque chose de nouveau à l'écosystème blockchain en Afrique, le numérique et les formations en ligne. La vitesse compte souvent, mais le résultat aussi. Le but est d'innover, d'attirer, de soigner les membres de notre communauté, afin de pouvoir construire un service durable et qui fera ensuite notre fortune. Certains acteurs que nous allons former, pourront être recrutés par POSITIVE INTERNET SOLUTION afin de nous aider à développer nos projets blockchain. Dans l'ensemble, toute la communauté de POSITIVE ACADEMY se tiendra prêt pour apporter sa valeur ajoutée à la construction de l'économie africaine de demain à l'aide du numérique.

