Quentin DEMÉ
Kévin RICOULT

100 MOTS pour COMPRENDRE les CRYPTOMONNAIES

GERESO

GERESO
FORMATION | CONSEIL | ÉDITION

100 mots pour comprendre les cryptomonnaies

100 MOTS POUR COMPRENDRE
LES CRYPTOMONNAIES

Auteurs : Quentin DEMÉ - Kevin RICOULT

Édition 2024

Direction de collection : Catherine FOURMOND
Suivi éditorial et conception graphique : GERESO Édition
Illustration : Benoît NAZARIN--PALAU

www.gereso.com/edition
e-mail : edition@gereso.fr
Tél. 02 43 23 03 53

Dépôt légal : Septembre2024
ISBN : 979-10-397-1001-5
EAN 13 : 9791039710015
ISBN numériques
ISBN eBook : 979-10-397-1268-2
ISBN ePub : 979-10-397-1269-9

GERESO SAS au capital de 465920 euros - RCS Le MANS B 311 975 577
Siège social : 38 rue de la Teillaie - CS 81826 - 72018 Le Mans Cedex 2 - France

Les « Hors Collection » GERESO Édition :

- Créer un site internet sans coder
- Guide juridique de l'entrepreneur rebelle au droit
- Guide pratique du cahier des charges informatique
- Je veux être un salarié heureux !
- L'entreprise à ciel ouvert
- L'entreprise désirable
- La gestion en restauration
- La vente éthique et bienveillante
- Le guide du Community Manager
- Le guide du petit entrepreneur
- Le pouvoir des images en formation
- Les rites et rituels professionnels
- Les holdings
- Organiser et réussir vos événements
- Petite entreprise, grands réseaux
- Piloter un projet industriel
- Prendre des notes avec le mind mapping
- Restez connecté !

Retrouvez tous nos titres « Hors Collection » sur
librairie.gereso.com

Librairie
GERESO

Sommaire

Introduction

Depuis plusieurs années, les cryptomonnaies ont pris une importance capitale dans l'économie mondiale, jusqu'à faire régulièrement la une de journaux financiers mondialement connus. Les gouvernements, les institutions, les entreprises et les particuliers leur accordent désormais une place de choix dans leurs réflexions. Malgré tout, la connaissance du grand public reste encore très restreinte, souvent circonscrite à quelques notions de base, constituant souvent la principale cause de défiance envers ce secteur.

Nous avons donc souhaité rendre accessible à tous cet univers complexe et fascinant, dans un format très facile d'accès et ludique. Ainsi, nous invitons le lecteur à découvrir ou redécouvrir cet écosystème, à travers 100 mots emblématiques, rangés par chapitre, dans l'ordre alphabétique.

Dans cet ouvrage, nous nous adressons à tous ceux qui souhaitent saisir les enjeux de ce nouveau paradigme. En priorité les débutants, qui trouveront au cours de leur lecture toutes les clés essentielles pour comprendre et démystifier le jar-

gon technique, mais également les connaisseurs pour qui ce livre sera une occasion d'approfondir leur compréhension.

Pour cela, nous proposons deux grilles de lecture différentes. Le lecteur curieux pourra se référer aux différents chapitres et se promener d'un terme à l'autre grâce aux références indiquées au sein de l'ouvrage, rendant sa découverte dynamique. Le lecteur pratique, qui souhaite utiliser notre ouvrage comme un soutien dans ses recherches, pourra se référer au glossaire présent en fin d'ouvrage.

Durant tout notre travail de recherche et de rédaction, nous n'avons eu de cesse que de répondre à cette ambition d'universalité, tout en étant sur une ligne de crête, afin de proposer un ouvrage qui soit simple d'accès sans être simpliste, vulgarisant les notions sans les approximer.

Ce livre est issu d'un double regard. Celui d'un universitaire, permettant de mettre en perspective cet écosystème avec les mécanismes à l'œuvre dans l'économie et de proposer une assise théorique solide. Celui d'un praticien, d'un connaisseur de ce qui se joue au niveau de la communauté des investisseurs, permettant de sélectionner les mots les plus pertinents et ainsi traduire des tendances de fond représentatives de la réalité du terrain.

Que ce soit pour investir en toute confiance, comprendre les implications technologiques ou simplement rester informé sur les évolutions économiques et financières en cours, cet ouvrage se veut être une ressource indispensable.

En espérant que vous prendrez autant de plaisir (mais moins de temps !) à lire cet ouvrage que nous en avons pris à l'écrire. Nous vous remercions pour votre confiance.

Chapitre 1

Les essentiels à comprendre avant de se lancer

L'écosystème des cryptoactifs regorge de termes techniques, souvent des anglicismes, qui peuvent parfois être difficiles à comprendre au premier abord. Nous avons proposé dans ce chapitre une compilation des mots les plus importants vous permettant de survivre dans cette jungle littéraire.

1 Airdrop

Signifiant « largage », l'***airdrop*** est une pratique qui consiste, pour une entité, à **distribuer une partie de ses actifs** à des individus identifiés selon certains critères, **sans contrepartie financière**.

Cette pratique peut répondre à plusieurs objectifs :

1. Faire connaître le projet ou l'entreprise.
2. Augmenter le nombre d'utilisateurs de la solution proposée contribuant ainsi au développement de son adoption par l'effet de réseau.
3. Récompenser les primo-participants pour leur implication dans le projet.

Il existe différents types d'***airdrop*** :

1. **L'*airdrop* ouvert** : le participant doit s'enregistrer sur le site de l'organisation ou du projet pour recevoir un nombre prédéfini de *tokens* (→ 19).
2. **L'*airdrop* sur snapshot** : le nombre d'actifs offerts est défini via la mesure à un instant donné de la quantité d'actifs détenus sur un portefeuille spécifique. La règle de distribution peut varier, mais celle du 1 pour 1 est la plus courante : pour chaque unité possédée lors du snapshot, l'utilisateur obtient une unité lors du ***airdrop***.
3. **L'*airdrop* communautaire** : les *tokens* sont distribués aux utilisateurs selon leur investissement sur les réseaux sociaux. Il peut être demandé de suivre le compte de l'organisation ou de reposter des informations.

Altcoin 2

Contraction du terme *alternative coin* signifiant « pièce de monnaie alternative », un ***altcoin*** désigne **n'importe quel cryptoactif autre que *bitcoin*** (→ 3).

Les ***altcoins*** se développent depuis plusieurs années et représentent, en mars 2024, une capitalisation de plus de 1 265 milliards d'euros, soit 48 % de la capitalisation totale du marché des cryptoactifs. L'***altcoin*** le plus important est aujourd'hui l'*ether*, la cryptomonnaie native *d'Ethereum* (→ 8), deuxième en matière de capitalisation avec près de 426 milliards d'euros.

3 Bitcoin

Ce terme recouvre en réalité deux notions souvent confondues :

1. ***Bitcoin*** avec une majuscule, qui désigne la blockchain.
2. ***bitcoin*** avec une minuscule, qui désigne la cryptomonnaie utilisée sur cette dernière.

Le nom de ***bitcoin*** est un mot-valise formé à partir de *bit* qui désigne en informatique l'unité binaire 0 ou 1 et *coin* qui signifie « pièce de monnaie ».

Bitcoin **est une blockchain créée en 2008** par un individu ou un groupe d'individus se présentant sous le pseudonyme de Satoshi Nakamoto. Depuis la création du ***bitcoin***, l'identi-té du ou des créateurs demeure une énigme.

Bitcoin se base sur les technologies de la *cryptographie* (→ 57) et de la *blockchain* (→ 4) afin d'assurer sécurité et transparence à l'ensemble du réseau. Depuis sa création, la blockchain ***Bitcoin*** n'a jamais été compromise.

Celle-ci est constituée de blocs liés les uns aux autres recensant l'ensemble des transactions entre les individus sur le réseau.

Le ***bitcoin*** **est la principale monnaie numérique du marché des cryptoactifs**. Sa capitalisation est de plus de 1 375 milliards d'euros, ce qui représente environ 52 % de la capitalisation totale du marché des cryptomonnaies en mars 2024. Sur les plateformes d'échange, le ***bitcoin*** est abrégé en BTC ou parfois XBT.

La création monétaire du ***bitcoin*** ne se réalise pas via une banque centrale comme pour les monnaies traditionnelles, mais selon des règles mathématiques précises. En effet, le protocole est conçu pour que la création de nouvelles unités monétaires se réalise de manière fixe et prédéterminée. L'offre totale est fixée à 21 millions et a été définie à la création de cette cryptomonnaie. Actuellement, plus de 90 % des ***bitcoins*** ont été créés par le processus de *minage* (→ 11), soit près de 20 millions d'unités. On estime que 99 % des ***bitcoins*** seront minés en 2034 et que la dernière unité sera minée en 2140.

Cette différence fondamentale avec les monnaies traditionnelles justifie que l'on qualifie ***bitcoin*** de monnaie « déflationniste », contrairement aux monnaies dites « inflationnistes » dont la quantité n'est pas limitée, à l'instar de l'euro ou du dollar.

Le processus de création de ***bitcoins*** se réalise de la manière suivante :

1. Lorsqu'une transaction en ***bitcoins*** intervient entre deux individus, celle-ci est intégrée dans un bloc avec d'autres transactions.

2. La validation du bloc et de ses transactions est réalisée en suivant un processus appelé « preuve de travail » ou *Proof Of Work* (→36). Ce processus consiste en la résolution d'un problème mathématique complexe nécessitant une grande puissance de calcul informatique.
3. Lorsque la solution est trouvée, le bloc est validé et chaîné avec les autres. Cette résolution donne lieu à une récompense pour le validateur du bloc sous la forme de ***bitcoins***. C'est ainsi que sont générées ces nouvelles unités.

En moyenne, un bloc est validé et intégré à la blockchain toutes les dix minutes, il y a donc une création monétaire à un rythme constant. En revanche, la masse monétaire créée est décroissante, car la récompense pour la validation d'un bloc diminue. Initialement fixé à 50 ***bitcoins***, le protocole ***Bitcoin*** prévoit de réduire de moitié la récompense tous les 210 000 blocs, soit tous les quatre ans environ. Ainsi, la récompense de bloc est passée de 6,25 ***bitcoins*** en 2023 à 3,125 en avril 2024.

Blockchain 4

Ce terme est l'un des termes les plus essentiels à définir dans le cadre de nos recherches, car cette technologie est centrale dans l'écosystème des cryptomonnaies.

Signifiant « chaîne de blocs », une ***blockchain*** est une **technologie de stockage d'informations et de transmission de valeurs**. À ce titre, elle est souvent comparée à un grand livre de comptes public, pseudonyme et infalsifiable.

En réalité, la ***blockchain*** utilise un ensemble de technologies combinées : une base de données (assurée par les blocs), un système d'historisation (l'enchaînement des blocs), un mode de transmission de l'information (via le réseau distribué) et une couche de sécurisation (via la cryptographie).

Même si le terme s'est réellement démocratisé ces dernières années, le concept de la technologie ***blockchain*** date en réalité des années quatre-vingt et est le fruit de plusieurs réflexions :

1. **Sur la sécurisation** : David Chaum, un informaticien américain qui a développé en 1982 un système de monnaie digitale appelée Digicash. Ce système permettait de réaliser des transactions anonymes grâce à la cryptographie.
2. **Sur l'historisation** : une étude en 1991 sur les chaînes de blocs cryptographiquement sécurisées est proposée par Stuart Haber et W. Scott Stornetta avec pour objectif de créer un système dans lequel des documents peuvent être horodatés et infalsifiables.

3. Sur l'application pratique : apparue en 2008 avec Bitcoin, elle devient un élément fondamental servant de registre public à toutes les transactions sur le réseau.

Ce mot provient de la manière dont le réseau stocke les données relatives aux transactions, c'est-à-dire des blocs (*block* en anglais), reliés pour former une chaîne (*chain* en anglais). La « chaîne de blocs » s'étend ainsi au fur et à mesure de l'augmentation du nombre de transactions. Les blocs recueillent et confirment les heures et les séquences des transactions. Ils sont consignés dans la ***blockchain*** selon des règles convenues entre ses membres.

Le fonctionnement simplifié de la ***blockchain*** en quatre étapes :

1. Lorsqu'une transaction est réalisée entre deux individus, elle est ajoutée aux autres dans un bloc.
2. Les *nœuds* (→ 33) du réseau vérifient la transaction et s'assurent que les individus en sont bien à l'origine.
3. L'ajout du bloc à la chaîne passe par la validation des membres du réseau, appelés mineurs, à travers un *mécanisme de consensus* (→ 32). Ces méthodes diffèrent selon les ***blockchains***, les deux plus utilisées étant le *Proof Of Work* (→ 36) et le *Proof Of Stake* (→ 35).
4. Une fois le bloc validé, celui-ci est ajouté à la ***blockchain*** existante et est partagé à l'ensemble du réseau pour que chacun actualise sa nouvelle version du registre.

Évidemment, le fonctionnement est plus complexe que celui décrit, mais tout au long de votre lecture, vous ajouterez et préciserez ces étapes qui, *in fine*, vous permettront d'appréhender techniquement son fonctionnement.

Pour bien comprendre les enjeux liés à cette technologie, il est essentiel d'évoquer un point conceptualisé par Vitalik Buterin, le cofondateur d'*Ethereum* (→ 8) : **le trilemme de la *blockchain*.** Ce dernier explique l'équilibre nécessaire entre trois notions paradoxales :

1. **La sécurité** : le réseau doit pouvoir prendre en compte des transactions sans que celles-ci soient modifiables, en les vérifiant pour s'assurer de leur authenticité, et en prévenant les attaques.
2. **La décentralisation** : le réseau doit être suffisamment autonome pour ne pas être assujetti à un organe central.
3. **La scalabilité** : la vitesse et les frais de transactions doivent évoluer de manière harmonieuse indépendamment du nombre d'utilisateurs.

Les exemples de ce trilemme sont légion. La ***blockchain*** Bitcoin par exemple est un modèle de décentralisation et de sécurité, mais comporte toujours des soucis de scalabilité. Le *Lightning Network* (→ 31) vise à résoudre ce problème.

5 Coin

De nombreux débats interviennent sur la définition précise d'un ***coin*** et les différences avec d'autres termes, tels que *cryptomonnaie* (→ 6) ou *token* (→ 19). Nous souhaitons proposer, dans cette définition, un cadre théorique qui permettra d'apporter des éléments de réponse qui seront bouleversés par la rapide évolution du cadre technologique de cet écosystème.

Signifiant « pièce », un ***coin*** désigne la **monnaie numérique native émise sur une blockchain** permettant de réaliser des transactions sur celle-ci. Parfois, le terme de *token* est utilisé comme synonyme de ***coin*** à tort. En effet, un *token* est, quant à lui, émis sur une blockchain déjà existante. C'est par exemple le cas de *l'altcoin* (→ 2) USDT du projet Tether USD émis sur Ethereum dont le ***coin*** est l'ether. Le terme cryptomonnaie est, quant à lui, utilisé pour désigner indifféremment des actifs numériques (qu'ils soient des ***coins*** ou des *tokens*).

Les ***coins*** sont donc les actifs émis par et sur une blockchain et sont nécessaires au bon fonctionnement de celle-ci. Ils peuvent avoir plusieurs usages. À titre d'exemple, un utilisateur souhaitant créer et exécuter un *smart contract* (→ 17) sur la blockchain Ethereum devra payer des frais de fonctionnement via le ***coin*** natif de celle-ci : l'ether (ETH). Ce *smart contract*, mis en fonctionnement sur Ethereum, peut à son tour proposer des services financiers qui nécessitent cette fois-ci l'émission d'un *token*.

Cryptomonnaie 6

Les ***cryptomonnaies*** désignent **tous les actifs numériques qui s'appuient sur la technologie de la blockchain pour être conservés et transférés**. On les appelle parfois « monnaie virtuelle » ou « monnaie numérique ».

Pour être très précis d'un point de vue économique, l'utilisation du terme « ***cryptomonnaie*** » pour désigner ces actifs est un peu trompeuse. Il serait plus exact de parler de « cryptoactifs ».

En effet, pour qu'une monnaie soit considérée comme telle, il faut qu'elle remplisse trois fonctions économiques essentielles :

1. **Intermédiaire des échanges** : elle doit permettre l'achat de biens et de services.
2. **Unité de compte** : elle sert d'étalon pour comparer le prix des biens et services.
3. **Réserve de valeur** : elle doit pouvoir être conservée dans le temps sans risquer de perdre sa valeur.

Les ***cryptomonnaies*** actuellement en circulation ne remplissent que partiellement ces trois fonctions :

1. **Intermédiaire dans les échanges** : selon l'article L. 111-1 du Code monétaire et financier « La monnaie de la France est l'euro », c'est la seule monnaie qui a un cours légal en France. C'est-à-dire que l'euro est accepté par tous comme moyen de paiement. Les cryptoactifs quant à eux n'ont pas cours légal. Ainsi, personne n'est obligé de les accepter comme moyen de paiement.

2. **Unité de compte** : afin de pouvoir comparer la valeur des biens à disposition, la valeur de la monnaie doit être relativement stable dans le temps. Les cryptoactifs ne remplissent pas ce rôle, car ils sont très volatils.
3. **Réserve de valeur** : la monnaie peut être épargnée pour un usage futur. La *volatilité* (→83) importante des actifs rend difficile cette fonction.

Malgré ces précisions, l'ensemble de la communauté et des médias utilisent le terme de « ***cryptomonnaie*** ». Par commodité, nous pourrons également employer ce mot dans notre ouvrage.

Il existe de nombreuses ***cryptomonnaies*** à travers le monde. Il est difficile de définir avec précision leur nombre tant la création et la disparition de certains actifs se font récurrentes. Néanmoins, nous estimons à 25000 le nombre de cryptoactifs en circulation. Malgré ce chiffre impressionnant, environ 70 % de la capitalisation totale du marché des ***cryptomonnaies*** est concentré sur seulement deux actifs : le bitcoin et l'ether.

Decentralized Finance (DeFi) 7

Signifiant « Finance décentralisée », la ***DeFi*** désigne, de manière générique, **l'ensemble des services financiers proposés sur la technologie *blockchain*** (→ 4).

Concrètement, la ***DeFi*** offre la plupart des services bancaires et financiers connus dans la finance classique, avec une distinction majeure : elle ne nécessite pas d'intermédiaire. Elle permet en effet les échanges de *pair-à-pair* (→ 61) de manière anonyme.

Quelques exemples de services proposés dans la ***DeFi*** :

1. **Prêts :** vous prêtez vos actifs financiers à d'autres utilisateurs et percevez des intérêts et des récompenses en retour. Aave est un exemple de plateforme qui propose ce type de service. Vous trouverez des explications plus détaillées au mot *lending* (→ 50).
2. **Emprunts :** en contrepartie du dépôt d'un séquestre (ou collatéral) en cryptoactifs, vous pouvez emprunter des actifs pour une valeur inférieure à celui-ci et payer des intérêts calculés sur la durée et le montant de l'emprunt. Compound est un exemple de plateforme proposant ce type de service.
3. **Épargne et placements :** vous placez votre capital sur des comptes rémunérés qui génèrent des intérêts à intervalles réguliers (quotidien, hebdomadaire ou mensuel). Bitstack est un exemple d'application qui propose ce type de placements.

La ***DeFi*** fonctionne grâce à la technologie blockchain et s'appuie sur les *smart contracts* (→ 17) permettant de sécuriser les transactions sans l'intervention d'intermédiaire. Les plateformes ***DeFi*** se présentent souvent sous la forme d'applications décentralisées ou *Dapps* (→ 40).

Au regard de son historique, de son efficacité et de sa simplicité d'accès, c'est la blockchain Ethereum qui concentre la majorité des services ***DeFi***.

Ethereum 8

Ethereum est une blockchain publique conçue pour le **déploiement de *smart contracts* et d'applications décentralisées**. **L'ether (ETH) est la cryptomonnaie native de ce réseau**. À l'heure de l'écriture de ces lignes, la capitalisation de celle-ci est la deuxième plus importante de l'écosystème, après le bitcoin.

Le projet ***Ethereum*** a été instauré par Vitalik Buterin en 2013 avec pour ambition de résoudre certains problèmes du réseau Bitcoin. En 2014, la fondation ***Ethereum*** a été créée pour organiser le développement du projet et près de 18 millions de dollars ont été récoltés. **Ce projet a été lancé publiquement en juillet 2015**.

Son apport fondamental est d'offrir des possibilités plus grandes que le simple transfert de valeur permis jusqu'alors par Bitcoin. Ce réseau a ouvert la voie à la finance décentralisée à travers l'implémentation des applications décentralisées, construites à partir de contrats intelligents.

Tous les utilisateurs peuvent ainsi s'appuyer sur ***Ethereum*** pour offrir des services divers : prêts, conversion, assurances. Pour fonctionner, ces services proposent des jetons ou *tokens* (→ 19) spécifiques. Ces jetons doivent répondre à une norme définie par le réseau ERC-20 permettant l'interopérabilité des services sur la blockchain ***Ethereum***.

Pour faire fonctionner le réseau et rémunérer les acteurs contribuant à sa sécurité, ***Ethereum*** utilise ce que l'on appelle le *gas* (→ 44). Chaque utilisateur devra s'acquitter d'une certaine somme en Ether pour utiliser des services sur la blockchain, cette somme est définie selon la complexité informatique de l'action souhaitée.

À sa création, le réseau ***Ethereum*** fonctionnait en *Proof Of Work* (→ 36), soit le même mécanisme de consensus que Bitcoin, qui a l'inconvénient d'être très coûteux en énergie et en infrastructures. Depuis « *The Merge* » en 2022, **le réseau utilise désormais le mécanisme de *Proof Of Stake*** (→ 35).

Ne souhaitant pas surcharger notre lecteur d'une définition trop longue, nous préférons lui apporter les éléments essentiels qui, accompagnés des autres définitions, lui donneront toutes les clés pour comprendre les bases de la révolution ***Ethereum***.

Exchange (CEX, DEX) 9

Signifiant « plateforme d'échange », un ***exchange*** est une **plateforme qui permet principalement l'achat et la vente d'actifs.** Dans l'écosystème des cryptomonnaies, il existe plus de 300 plateformes proposant une multitude de services complémentaires à l'achat et la vente d'actifs tels que le *staking* (→ 51), le *lending* (→ 50) ainsi que la gestion de son portefeuille.

Il existe **deux catégories de plateforme d'échange**, les centralisées (***CEX***) et les décentralisées (***DEX***) :

1. Les ***CEX*** sont l'abréviation de *Centralized Exchange* signifiant « plateformes d'échange centralisées ». Celles-ci sont créées et gérées par une entreprise privée, d'où la notion de centralisation. Elles constituent la majorité des plateformes d'échange connues dans l'écosystème des cryptomonnaies. En effet, par leur simplicité d'utilisation et d'accès, elles permettent aux nouveaux investisseurs d'utiliser intuitivement une interface pour entamer leurs premiers investissements. Ces plateformes doivent être approvisionnées en monnaie fiduciaire (euro ou dollar par exemple) par carte bancaire, virement SEPA ou via un compte *Paypal*.
2. Les ***DEX*** sont l'abréviation de *Decentralized Exchange* signifiant « plateformes d'échange décentralisées ». Ne nécessitant pas d'organe central, les ***DEX*** ont des contraintes financières réduites par rapport aux ***CEX***. Les plateformes décentralisées offrent donc des frais de tran-

sactions plus faibles, permettant une rentabilité plus élevée. Néanmoins, ce type de plateforme d'échange n'offre pas la possibilité de transférer directement des monnaies fiduciaires. Il est donc nécessaire d'effectuer en amont une conversion de monnaie *fiat* (→ 94) vers un actif qui sera utilisé sur le ***DEX***. Les plateformes décentralisées ne conservent pas les fonds des utilisateurs qui restent responsables de leur stockage.

Nous présentons ci-après les principaux inconvénients de chaque type de plateforme :

1. Puisque centralisées, les ***CEX*** accroissent le risque de cyberattaques ciblées visant à extorquer les fonds stockés par les entreprises. Elles ont également des coûts de transactions supérieures aux ***DEX*** en raison de leurs coûts de structure.
2. Les plateformes d'échange décentralisées souffrent de deux défauts majeurs : une faible *liquidité* (→ 75) des actifs proposés ainsi que la mauvaise expérience utilisateur de leurs interfaces, peu intuitives et peu faciles d'accès aux néophytes.

Métavers 10

Contraction de « méta » et « univers » signifiant « au-delà de l'univers », le ***métavers*** désigne un **réseau d'écosystèmes virtuels qui permet l'interaction entre les utilisateurs et leurs environnements**, offrant une expérience à mi-chemin entre le réel et le virtuel. Ce terme peut également être rencontré dans sa version anglaise *metaverse*.

Le ***métavers*** permet principalement aux utilisateurs particuliers ou professionnels de s'immerger à travers un avatar dans un monde parallèle, simulant la réalité.

Nous présentons quelques applications permises par le ***métavers*** :

1. **Construire une vie sociale** : l'utilisateur évolue dans un monde virtuel à travers son avatar et peut reproduire une vie semblable à la réalité en interagissant avec d'autres individus.
2. **Expérimenter une vie culturelle et ludique** : l'utilisateur peut vivre des expériences telles que visiter un musée ou assister à des concerts.
3. **Participer à une vie économique** : les utilisateurs peuvent consommer un large choix de biens et services virtuels proposés par d'autres individus. Les transactions s'effectuent alors avec la monnaie virtuelle de la plateforme.

Cette révolution technologique est permise notamment par le *Web 3.0* (→ 22) et représente un véritable accélérateur pour l'écosystème des cryptomonnaies. Le ***métavers*** crée un réel engouement auprès des sociétés technologiques

convaincues qu'un nouveau modèle économique émerge. À ce jour, les principaux acteurs sont *The Sandbox* et *Decentraland*.

La simulation du réel permis dans le ***métavers*** est très importante : il est possible d'acheter des vêtements exclusifs pour son avatar, proposés dans des magasins virtuels par des marques célèbres telles que Louis Vuitton. Il est également possible de devenir propriétaire de terrains ou de maisons vendus par des professionnels. Comme dans le monde réel, ces derniers ont plus ou moins de valeur selon leurs emplacements, c'est notamment le cas de certains terrains acquis en 2021 jusqu'à 458 000 $ à proximité de ceux du rappeur Snoop Dogg. Enfin, des influenceurs virtuels à l'instar de Lil Miquela proposent des partenariats avec des marques luxueuses comme Calvin Klein ou Prada.

Le ***métavers*** permet également des interactions fortes entre réel et virtuel : en avril 2022, le PDG de Carrefour annonçait faire passer ses premiers entretiens d'embauche pour des postes de *data analyst* dans le monde virtuel The Sandbox.

Minage 11

Dans le secteur des cryptomonnaies, le ***minage*** est une **étape primordiale et essentielle contribuant à la sécurité et l'intégrité des réseaux**. Il est important de rappeler que le terme « ***minage*** » ne convient que pour les blockchains utilisant le système de la preuve de travail ou *Proof Of Work* (→ 36).

Le ***minage*** est le processus qui permet de valider des informations et de les intégrer sous la forme d'un nouveau bloc de données, d'où le terme de *blockchain* ou « chaîne de blocs ». Les utilisateurs qui participent à ce processus sont appelés « mineurs ».

En pratique :

1. Dès qu'une transaction est réalisée sur un réseau *Proof Of Work*, les données sont enregistrées dans un bloc et transmises aux mineurs pour validation et intégration à la blockchain.
2. Chaque bloc à valider possède une empreinte numérique, également appelée *hash,* obtenue par une fonction mathématique de *hachage* (→ 27). Toutes les données du bloc (horodatage, transactions…) sont transformées par cette fonction et se traduisent par une chaîne de caractères (dite *hash*) unique.
3. Les mineurs vérifient les transactions réalisées au sein du bloc et l'intègrent à la chaîne. Pour cela, ils doivent trouver une solution à une équation mathématique. L'équation diffère selon les réseaux. Il peut par exemple s'agir d'obtenir un *hash* final qui débute par un nombre donné de 0.

4. Pour trouver la solution, les mineurs doivent trouver une chaîne de caractères, appelée *nonce* qui, ajoutée à l'empreinte numérique initiale du bloc, puis « hachée » par la fonction mathématique, donnera un *hash* final répondant aux spécifications demandées. Ces spécifications induisent un niveau de difficulté qui est dynamique et s'adapte en fonction de la puissance de calcul disponible sur le réseau afin d'assurer une validation de blocs constante dans le temps.
5. Comme la fonction mathématique de hachage est imprévisible, la seule méthode pour trouver la solution est par « brute force », c'est à dire le test de centaines de millions de *nonces* une à une jusqu'à obtenir le *hash* répondant aux spécifications. C'est ce processus de recherche qui se fait appeler le « ***minage*** ».
6. Dès que le *hash* est trouvé, le nouveau bloc est diffusé à l'ensemble du réseau pour être vérifié par d'autres nœuds puis est ajouté à la blockchain.

Pour inciter les utilisateurs à participer au processus de ***minage***, les mineurs sont récompensés financièrement dès qu'ils parviennent à valider un bloc. Pour la blockchain Bitcoin, un mineur obtient en 2024, 3,125 bitcoins pour chaque bloc validé.

Pour augmenter leur probabilité de trouver le *nonce*, les mineurs doivent augmenter leur puissance de calcul afin de tester un nombre plus important de *nonces.* La difficulté s'adaptant selon la puissance de calcul disponible, un mineur seul avec un simple ordinateur en 2024 n'a quasiment aucune chance de trouver la solution. Ainsi, la plupart des mineurs utilisent des outils plus puissants dédiés au ***minage***. Parfois, ils assemblent des centaines d'équipements dans un même espace appelé « ferme de ***minage*** ». D'autres s'organisent en

« pool de ***minage***», c'est-à-dire au sein d'un réseau organisé rassemblant plusieurs mineurs. Dans ces réseaux, chaque mineur travaille individuellement avec son équipement et lorsque l'un d'eux parvient à valider un bloc, il partage sa récompense avec l'ensemble du réseau. Cette méthode permet d'augmenter les chances de réussite.

La critique de Bitcoin et d'autres cryptomonnaies fonctionnant en *Proof Of Work* provient en partie de ce processus de ***minage***. En effet, celui-ci est énergivore et coûteux (matériel, électricité, espaces…). La puissance électrique qu'il demande au niveau mondial fait de ce mécanisme de consensus un inconvénient majeur et un point de critique écologique fort.

Des innovations technologiques se sont néanmoins développées pour améliorer l'efficacité et la rentabilité du ***minage***. Parmi celles-ci l'ASIC, acronyme d'*Application-Specific Integrated Circuit*, est un type de circuit électronique conçu pour exécuter une tâche spécifique, ici la résolution d'algorithmes mathématiques complexes. Cette innovation permet aux mineurs d'obtenir plus fréquemment des récompenses, mais représente une menace pour la décentralisation du réseau.

12 NFT (Non Fungible Token)

Signifiant « jeton non fongible », un ***NFT*** est un **actif numérique non interchangeable**.

Pour comprendre, il faut expliquer ce que l'on entend par « non fongible ». En économie, on parle de fongibilité d'un bien lorsque celui-ci peut être échangé par un autre de même genre sans distinction. Par exemple, la monnaie est un bien fongible, car nous pouvons échanger indifféremment un euro contre une autre pièce d'un euro.

Les ***NFT*** recouvrent plusieurs utilités :

1. **Fonctionnelle** : permettre l'accès à des événements à travers une preuve de possession.
2. **D'authentification** : prévenir la contrefaçon d'un bien et garantir l'authenticité d'un document.
3. **Communautaire** : offrir un avantage au détenteur du ***NFT***.
4. **Artistique** : créer et certifier des œuvres digitales (œuvres d'art, photos, vidéos, objets de collection).

Le PoAP (*Proof of Attendance Protocole*) signifiant « protocole de preuve de présence » est un parfait exemple d'usage fonctionnel des ***NFT*** dans le monde réel. Un PoAP est un ***NFT*** qui permet de certifier la présence à un événement. Les organisateurs peuvent décider de créer ce ***NFT*** pour permettre à leurs participants de garder un souvenir de l'événement, infalsifiable et propre à chacun.

Les ***NFT*** offrent la possibilité de répliquer le conceptd'unicité sur Internet grâce aux *smart contracts* (→ 17). Ainsi, il est possible de déterminer l'auteur d'une œuvre digitale, de lui associer des droits et de transmettre sa propriété à des acheteurs qui peuvent vérifier son authenticité.

Le premier ***NFT*** a été créé en 2014 et est attribué à l'artiste Kévin McCoy. Il s'agissait d'une œuvre nommée *Quantum* représentant une animation en forme d'octogone. Les ***NFT*** ne se sont vraiment développés qu'à partir de 2017 parallèlement au développement de la blockchain Ethereum et du standard technique ERC-721. Le ***NFT*** le plus cher de l'histoire est une œuvre d'art nommée *Every days – The first 5000 days* par l'artiste Mike Winkelmann qui s'est vendue à 69,3 millions de dollars. En 2022, les ventes de ***NFT*** représentaient 24,8 milliards de dollars.

13 P2E (Play to Earn)

Signifiant «jouer pour s'enrichir», le ***Play to Earn*** offre une **nouvelle expérience de gaming permettant aux joueurs d'obtenir des récompenses sous forme de cryptoactifs** au cours de leur évolution. Ce terme peut également être rencontré dans sa version abrégée ***P2E***.

Ce concept s'est démocratisé en 2017 grâce au développement de la blockchain Ethereum. À ce jour, le projet Axie Infinity est le plus connu (même si ce dernier n'utilise désormais plus Ethereum). Il s'agit d'un jeu basé sur l'élevage de monstres destinés à combattre et qui permet de gagner des actifs (AXS) et des NFT pouvant être revendus.

Le nouvel *ATH* (→89) du Bitcoin en 2021 a suscité un engouement populaire autour des cryptomonnaies, profitant ainsi aux marchés des NFT et du ***Play to Earn***. Le nombre de joueurs est alors passé de 58000 en 2021 à 1,17 million au premier trimestre 2022. La capitalisation totale du ***Play to Earn*** est d'environ 17 milliards d'euros à l'heure de l'écriture de ces lignes.

Apprécié comme nouvelle source de revenus pour certains, le ***Play to Earn*** est critiqué par d'autres qui estiment qu'il dénature le concept originel des jeux vidéo, à savoir jouer pour le plaisir. Dans cette logique, une nouvelle ère de jeux se développe sur la blockchain : le *Play to Enjoy*.

Registre distribué 14

Un ***registre distribué***, également appelé *Distributed Ledger*, est un **ensemble de données enregistrées, partagées et synchronisées par des utilisateurs sur un réseau décentralisé**. Il permet d'enregistrer des transactions telles que l'échange d'informations ou d'actifs entre les participants du réseau.

Contrairement à une base de données traditionnelle, ces registres ne contrôlent ni les données ni la gestion de celles-ci permettant ainsi d'accélérer les transactions. La transparence est assurée par la redondance des informations détenues par l'ensemble des participants, favorisant la sécurité et limitant la manipulation ou l'attaque du système. Fonctionnant sur un réseau *pair-à-pair* (→ 61) sans administrateur, c'est donc grâce à un *mécanisme de consensus* (→ 32) que le bon fonctionnement est assuré.

La technologie de ***registre distribué*** la plus connue est la blockchain qui par sa décentralisation via les nœuds, son mécanisme de consensus, la structure d'une chaîne de blocs et l'utilisation de la cryptographie répond parfaitement aux caractéristiques d'un ***registre distribué*** : sécurité, transparence, résilience et efficacité.

15 Roadmap

Signifiant « feuille de route », la ***roadmap*** est le **fil conducteur d'un projet** permettant à un utilisateur de connaître les différentes étapes de développement ainsi que leurs échéances.

La ***roadmap*** est généralement représentée sous forme d'organigramme et peut être intégrée au *white paper* (→ 23). Elle peut également servir d'argument pour les investisseurs et les parties prenantes, en démontrant une vision et un plan clairement établi pour atteindre des objectifs temporels et mesurables. Enfin, cette feuille de route permet à l'équipe de développement de s'interroger sur sa capacité à atteindre les objectifs et d'estimer sa charge de travail et par conséquent le coût du processus.

La ***roadmap*** contient les informations essentielles sur le déploiement du projet :

1. Une présentation générale de la solution.
2. Les grandes étapes d'évolution du projet et leurs échéances prévisionnelles de réalisation.
3. Les phases de tests permettant le passage aux prochains jalons.
4. La date officielle de lancement.

Lorsque les délais annoncés ne sont pas respectés ou que les phases de tests ne sont pas concluantes, on observe généralement une baisse de la confiance des investisseurs conduisant ainsi à une dépréciation du projet. À l'inverse, lorsque la ***roadmap*** est parfaitement suivie, la communauté sera mise en confiance impactant positivement le cours de l'actif.

Shitcoin 16

Signifiant « pièce de merde », le terme ***shitcoin*** est un attribut qui désigne **un actif sans réelle valeur technologique ni projet fondé** et qui parfois relève même de l'escroquerie.

La multiplication des ***shitcoins*** ces dernières années s'explique par le développement massif de la spéculation financière et la réussite de certains projets sans réelle valeur technologique. Ces derniers ayant parfois obtenu des rendements très importants, notamment à la suite de leur mise en avant par des personnalités influentes. Le *Doge Coin* est un des exemples les plus connus dont le cours a augmenté de près de 800 % en un mois, après les déclarations du milliardaire Elon Musk.

Évidemment, les ***shitcoins*** ayant permis un enrichissement représentent une part infinitésimale en comparaison de ceux ayant occasionné des pertes très importantes. Il est donc important de savoir reconnaître ce type de projets, notamment grâce à l'*analyse fondamentale* (→ 66).

17 Smart contract

Signifiant « contrat intelligent », un ***smart contract*** est un **protocole informatique qui permet d'exécuter des instructions selon des règles prédéfinies par les parties** et qui s'appuie sur la technologie de la *blockchain* (→ 4) pour garantir son inviolabilité.

Le concept de ***smart contract*** est apparu dès 1996 avec les réflexions de Nick Szabo, un informaticien à l'origine d'un des premiers projets de monnaie numérique décentralisée : le Bit Gold.

En pratique :

1. Une entreprise souhaite proposer une assurance pour le retard d'un avion. Pour cela, les parties s'accordent en amont sur les termes de l'assurance qui revêt la forme d'un ***smart contract*** intégré à une blockchain afin d'assurer son inviolabilité, c'est-à-dire que l'on ne pourra pas modifier les termes du contrat *a posteriori*.
2. Le contrat qui fonctionne sans l'intervention des parties vérifie les données aéroportuaires concernant les heures d'arrivées des avions par le biais d'un outil informatique appelé *oracle* (→ 34).
3. Si les données récoltées montrent un retard de l'avion, le ***smart contract*** déclenche le remboursement de l'usager.

Avec un *smart contrat*, le fonctionnement est simplifié pour tous et offre deux bénéfices majeurs au consommateur : un délai et un coût considérablement réduits. En effet, avec une assurance traditionnelle, si l'avion avait eu du retard, une

réclamation manuelle avec l'ensemble des justificatifs aurait été demandée nécessitant plusieurs vérifications de l'organisme afin de s'assurer de l'éligibilité au remboursement. L'assureur aurait par la suite envoyé l'instruction à sa banque de procéder au virement, permettant au consommateur de recevoir quelques jours plus tard l'indemnisation. Dans notre scénario, les justificatifs sont remplacés par les données certifiées exactes provenant de l'oracle et la réclamation manuelle par l'action de déclenchement du ***smart contract*** de l'une des deux parties (le consommateur).

Aujourd'hui, les ***smart contracts*** sont utilisés dans de nombreux domaines tels que la finance décentralisée ou *DeFi* (→ 7), les *NFT* (→ 12), la *supply chain*, et la plupart sont intégrés dans la blockchain *Ethereum* (→ 8). Ces derniers sont principalement écrits dans le langage informatique *Solidity* (→ 37).

Malgré ces perspectives intéressantes, ce type de contrat n'est pas sans risque. Si leur intégration dans la blockchain garantit leur inviolabilité, il n'est pas exclu qu'ils contiennent des failles conscientes ou inconscientes que des acteurs du marché malintentionnés peuvent exploiter pour extorquer de l'argent. C'est ce qu'il s'est passé en 2016 avec le projet The DAO qui a conduit à la disparition de l'équivalent de 50 millions de dollars.

18 Stablecoin

Signifiant « pièces de monnaie stables », **un *stablecoin* est un cryptoactif adossé à des valeurs ayant un cours constant** telles que des monnaies traditionnelles ou des actifs tangibles.

Le marché des cryptomonnaies est très volatil, ce qui peut constituer un frein et ralentir l'adoption de cette nouvelle technologie, notamment dans le cadre des échanges commerciaux. Les ***stablecoins*** se sont donc développés et permettent de répondre à ce besoin de stabilité des cours tout en conservant les avantages des cryptoactifs et de la technologie *blockchain* (→ 4).

Il existe deux principaux types de ***stablecoins***, l'un fonctionnant grâce à des réserves de valeur et l'autre grâce à des algorithmes.

La méthode des réserves de valeur recouvre quant à elle deux réalités différentes. Il peut s'agir de réserves dites *on chain* ou *off chain*, selon si les actifs répliqués sont présents ou non sur une blockchain.

Pour les premières, le ***stablecoin*** est adossé à d'autres actifs décentralisés. L'actif le plus connu utilisant ce mécanisme est le DAI.

Pour les secondes, le ***stablecoin*** est adossé à une valeur physique supposée stable telle qu'une monnaie fiduciaire ou un actif tangible comme l'or.

L'actif le plus connu utilisant ce mécanisme est le Tether (USDT) créé en 2014 qui réplique le dollar. Ce fonctionnement est le plus répandu dans l'industrie.

La méthode des algorithmes utilise quant à elle le fonctionnement économique de l'offre et de la demande. L'algorithme qui gère le ***stablecoin*** augmente ou réduit l'offre de monnaie selon la demande afin d'assurer la stabilité du prix. Si celui-ci est supérieur à une valeur de référence (dans la majorité des cas 1 $), le protocole augmente l'offre de monnaie afin de dévaluer le cours du ***stablecoin*** et le faire atteindre de nouveau la parité. À l'inverse, si le prix est inférieur, l'algorithme va réduire la masse monétaire.

À ce jour, nous comptons approximativement 200 ***stablecoins*** dans l'écosystème dont voici la liste des trois ***stablecoins*** principaux en mars 2024 avec leur capitalisation :

1. Tether (USDT), 103 milliards de dollars.
2. USD Coin (USDC), 30 milliards de dollars.
3. Dai (DAI), 5 milliards de dollars.

19 Token

Signifiant «jeton», le ***token*** désigne **un actif numérique non natif d'une blockchain**. Celui-ci ne fonctionne pas sur son propre réseau, mais s'appuie sur une chaîne de blocs préexistante. Celui-ci ne doit pas être confondu avec un *coin* (→ 5), émis au lancement d'une blockchain et nécessaire à son fonctionnement.

Nous vous proposons ci-après les principaux types de ***tokens*** :

1. **Les *utility tokens*** : ils permettent l'utilisation de services proposés par une entité grâce à une monnaie interne au projet, son ***token***. C'est par exemple ce que propose Filecoin avec «*FIL*» qui permet d'utiliser un réseau décentralisé de stockage de fichiers.
2. **Les *security tokens*** : ils sont générés lors d'une *STO* (→ 52), le *security* ***token*** est la représentation d'une part d'entreprise émise sur la blockchain. Il est considéré comme une valeur mobilière et doit donc répondre aux réglementations de cette catégorie d'actifs financiers imposées par les autorités financières.
3. **Les *fans tokens*** : ils sont utilisés pour développer un sentiment d'appartenance autour d'un projet et donner du pouvoir à leurs détenteurs. Ils offrent des droits de vote sur certaines décisions prises telles que le choix d'un nouveau design pour un logo, la sélection des joueurs ou encore l'esthétique de nouveaux maillots.
4. **Les *exchanges tokens*** : ils permettent l'utilisation des services proposés par les plateformes. Kucoin, avec son jeton «*KSC*» émis sur Ethereum, propose par exemple la

redistribution de dividendes aux détenteurs ainsi qu'une réduction de frais sur les transactions selon la quantité de ***tokens*** possédés.

Chaque ***token*** est unique et infalsifiable permettant ainsi le développement de la « tokenisation », à savoir la capacité d'attribuer une valeur à divers éléments physiques ou non. L'entreprise RealT propose par exemple l'achat de tout ou partie d'un bien immobilier dont le titre de propriété est représenté par un ***token*** qui donne lieu à des rentes.

L'ensemble des ***tokens*** en circulation forment la *circulating supply* qui se distingue de l'offre maximale d'un ***token*** également appelée *total supply*, tous les jetons n'étant pas nécessairement produits ou distribués à un instant donné.

20 Tokenomics

Contraction de *token* et *economics* signifiant « l'économie des jetons », la ***tokenomics*** est **l'étude des caractéristiques de création, de l'émission et de distribution de l'actif d'un projet**.

Étape incontournable de l'*analyse fondamentale* (→ 66), l'étude de la ***tokenomics*** regroupe l'analyse de multiples facteurs dont voici les plus importants :

1. **L'offre totale et son évolution :** nous pouvons retrouver deux évolutions drastiquement opposées de l'offre, inflationniste ou déflationniste. Semblable aux monnaies traditionnelles, l'offre inflationniste se caractérise par une offre en croissance perpétuelle. L'offre déflationniste se caractérise par la limite de la quantité d'actifs en circulation rendue possible, soit par l'imposition d'un nombre maximum d'actifs créés comme pour le bitcoin et ses 21 millions d'unités ou par un mécanisme de destruction périodique comme pour le BNB.
2. **La distribution** : le « lancement équitable » et le « lancement avec pré-minage » sont les deux modes de distribution explorés par la communauté jusqu'à présent d'un nouveau *token*. Le premier offre l'accès au jeton pour tous les acteurs du marché en même temps tandis que le second permet une première distribution aux investisseurs et créateurs du projet avant que l'accès soit rendu possible au public. Cette dernière présente un risque, si le *token* est distribué en grande quantité en amont à un collectif restreint, celui-ci pourra alors procéder à une vente massive impactant négativement le prix de l'actif.

3. **L'utilité** : les *tokens* répondant au mécanisme de l'offre et de la demande, plus un actif présente un intérêt pour ses utilisateurs, plus sa valeur a une probabilité d'être forte. Il convient donc de comparer la valeur du *token* à son utilisation afin d'estimer si celle-ci est sous ou surcotée.

Cette étude est essentielle, car la manière de gérer les *tokens* est un indicateur important pour le marché et peut impacter l'engouement des investisseurs et des parties prenantes.

21 Wallet

Signifiant « portefeuille », un ***wallet*** est un **portefeuille numérique qui permet de stocker vos cryptoactifs**.

Pour être très précis, ce ne sont pas vos actifs qui sont directement stockés dans ce portefeuille, mais vos *clés privées* (→ 55). Ce sont ces dernières qui vous permettent d'accéder à vos actifs.

En 2022, *Crypto.com* recensait plus de 425 millions détenteurs de cryptomonnaies à travers le monde, soit 5 % de la population mondiale.

Il existe deux grands types de portefeuille :

1. Les ***hot wallets*** : signifiant « portefeuilles à chaud », ce sont des solutions de stockage qui utilisent des appareils connectés à Internet. De ce fait, ces portefeuilles sont moins sécurisés et vos actifs sont plus vulnérables aux attaques. Parmi ces *hot* ***wallets***, il existe différentes solutions telles que les *web* ***wallets*** qui sont des portefeuilles accessibles à travers un navigateur (exemple : MetaMask), les *mobile* ***wallets*** qui se présentent sous la forme d'applications (exemple : Trust ***Wallet***) et les *desktop* ***wallets*** qui sont des logiciels pour ordinateur (exemple : Exodus).
2. Les ***cold wallets*** : signifiant « portefeuilles à froid », ce sont des solutions de stockage déconnectées. Puisque non connectées à Internet, ces solutions sont considérées comme les plus sûres. Parmi ce type de portefeuille, il existe également différentes solutions telles que les *hardware* ***wallets*** qui sont des portefeuilles physiques à

l'instar des clés *Ledger* (→ 59) ou les *paper* ***wallets*** qui désignent une solution basique constituant à inscrire sa clé privée et son adresse de détention sur un lieu physique de son choix.

Chaque type de portefeuille peut être utilisé complémentairement : les *hot* ***wallets***, plus rapides d'utilisation, renferment une partie des actifs utilisables pour des transactions régulières et les *cold* ***wallets***, plus sûrs, permettent de stocker une masse plus importante de cryptoactifs moins fréquemment mobilisés.

22 WEB 1.0/2.0/3,0

Le ***Web 1.0, 2.0*** et ***3.0*** désigne **trois générations de développement du *web***.

Avant toute chose, il convient de poser une distinction essentielle entre deux notions souvent confondues : Internet et le ***web***. Pour résumer simplement, Internet représente l'infrastructure et le ***web*** est un des services de cette infrastructure.

Abréviation de *Interconnected Network* signifiant « réseau interconnecté », Internet est une invention de l'armée américaine qui date des années soixante, bien avant le ***web***. De nombreuses applications peuvent être utilisées grâce à Internet telles que le réseau *pair-à-pair* (→ 61), les serveurs FTP, mais l'application la plus utilisée d'Internet est évidemment le ***web***.

Signifiant « toile », le ***web*** est un système interconnecté de pages reliées entre elles via des liens hypertextes. Pour gérer ces informations contenues dans les liens hypertextes, nous utilisons des navigateurs ***web*** tels que Chrome ou Safari.

Le concept du ***web*** a été proposé par Tim Berners-Lee, un employé du CERN (l'Organisation européenne pour la recherche nucléaire) dans les années quatre-vingt-dix.

Le ***Web 1.0*** est donc apparu et s'est développé au cours des années quatre-vingt-dix jusqu'au milieu des années deux mille. Il s'agissait d'un ***web*** avec une approche plutôt descendante : on pouvait **consulter des informations, mais on**

ne pouvait pas produire de contenus ou interagir. L'objectif de cette nouvelle technologie, que l'on nomme « ***web*** passif », est de transposer l'information physique en information virtuelle.

Puis le ***Web 2.0*** s'est développé, plus dynamique et participatif. Il permet la **production de contenus et le partage entre utilisateurs**, notamment avec l'apparition des premiers réseaux sociaux tels que Facebook en 2004 ou YouTube en 2005. Ce sont ces différentes nouveautés qui font du ***Web 2.0*** un environnement social et participatif.

Le ***Web 3.0*** ou ***Web3*** se veut être le successeur du ***Web 2.0*** en proposant une forme « décentralisée » permettant de proposer une alternative au système contrôlé par les GAMMA (Google, Apple, Meta, Microsoft et Amazon) et de redonner la possession de leurs contenus aux utilisateurs. Le terme ***Web3*** a été proposé par Gavin Wood en 2014, un informaticien ayant cofondé Ethereum. Le ***Web 3.0*** est pour le moment aux prémices de son développement, mais nous pouvons entrevoir ses opportunités : **les utilisateurs pourront être acteurs des évolutions des projets, reprendre le contrôle sur leurs données personnelles** et par exemple décider de les monnayer ou non. Le ***Web 3.0*** s'appuie donc sur la technologie *blockchain* (→4) et les *cryptomonnaies* (→6) pour proposer des nouveaux modèles de croissance actuellement basés sur la publicité dans le ***Web 2.0***.

Pour résumer, la distinction entre les différents ***Web 1.0, 2.0*** et ***3.0*** réside donc principalement dans le rôle des utilisateurs.

23 White paper

Signifiant «livre blanc», le ***white paper*** est un **outil d'information et de promotion d'un projet à destination de la communauté**. Ce recueil offre des informations essentielles sur l'origine du projet, son ambition, ses caractéristiques techniques, l'équipe de développement ainsi que sur la stratégie mise en place pour atteindre les objectifs établis.

Souvent rédigé et publié par l'initiateur du projet, le ***white paper*** est destiné à convaincre de l'intérêt du projet avec parfois l'ambition de lever des fonds auprès d'investisseurs via une *ICO* (→ 45) par exemple.

Le plus célèbre des ***white paper***s a été publié par Satoshi Nakamoto le 31 octobre 2008. Il décrit l'intérêt d'une monnaie décentralisée et propose une solution : le bitcoin. Un ***white paper*** n'est caractérisé par aucune norme de rédaction, il s'agit d'un document libre sans minimum de pages.

Le ***white paper*** est un document essentiel à consulter pour une *analyse fondamentale* (→ 66), il n'en est pas pour autant une preuve de solidité du projet. En effet, il n'est pas rare de voir des projets d'apparence sérieuse accompagnés d'un ***white paper*** complet se révéler être finalement un *scam* (→ 62). Il convient donc de ne pas juger le potentiel d'une nouvelle cryptomonnaie en fonction de ce seul document.

Chapitre 2

Le fonctionnement des technologies sous-jacentes

Grâce au chapitre 1, vous comprenez désormais les notions essentielles et avez fait les premiers pas dans ce monde complexe que sont les cryptoactifs. Au cours de votre lecture, vous avez pu remarquer que la plupart des notions font appel à des technologies et des concepts mathématiques parfois complexes. Ce chapitre a pour vocation de présenter ces éléments et d'expliquer leur fonctionnement.

24 Arbre de Merkle

Également appelé « arbre de hachage », l'***arbre de Merkle*** est une **structure destinée à sécuriser et compresser un ensemble de données en un seul point via un algorithme de *hachage*** (→ 27) cryptographique.

Techniquement, l'***arbre de Merkle*** se décompose de la façon suivante :

1. Les feuilles représentent une transaction dont chacune possède un *hash* d'identification unique.
2. Les *hashs* de deux transactions sont combinés pour donner un nouveau *hash* appelé sous-branche.
3. Les *hashs* des sous-branches sont concaténés jusqu'à l'obtention d'un nouveau *hash* appelé branche.
4. Les *hashs* des branches sont eux aussi concaténés jusqu'à obtenir deux derniers *hashs* appelés branches supérieures.
5. Les *hashs* des deux branches supérieures sont enfin combinés, créant ainsi le *hash* final appelé racine de Merkle.

Inventée par le cryptographe américain Ralph Merkle en 1979, cette architecture est fondamentale à la technologie blockchain puisqu'elle permet de prouver la validité des données en optimisant l'espace de stockage.

En effet, le *hash* final étant le résultat de multiples hachages des données, toute modification d'une simple transaction aurait pour conséquence de modifier fondamentalement la racine de Merkle. Grâce à cette structure, la vérification d'une transaction est simplifiée et accélérée et ne nécessite pas de télécharger l'intégralité de la base de données.

Bridge 25

Signifiant « pont », un ***bridge*** est un **protocole permettant la connexion entre différentes blockchains**. Sans elle, chacune demeure isolée et ne peut pas communiquer avec des projets présents sur d'autres blockchains.

Polkadot est l'un des protocoles précurseurs permettant à plusieurs blockchains d'être reliées et donc de communiquer des informations et réaliser des transactions entre elles. À titre d'exemple, ce protocole permet d'envoyer des ethers sur la blockchain Polkadot, c'est ce que l'on appelle l'interopérabilité.

En pratique, les actifs ne sont pas réellement transférés. Ils sont verrouillés via un *smart contract* (→ 17) sur la blockchain émettrice puis une copie est créée sur celle destinatrice, ce qui empêche l'utilisation de la cryptomonnaie sur les deux blockchains en simultané. Les copies créées correspondant au montant verrouillé sur la chaîne émettrice porteront généralement devant leurs abréviations le préfixe « *w* » pour *wrapped* signifiant « enveloppé ».

26 Burn

Signifiant «brûler», un ***burn*** est la **destruction intentionnelle d'une quantité d'actifs numériques** ayant pour objectif de réduire l'offre disponible.

Le marché des cryptomonnaies étant régi par la loi de l'offre et de la demande, l'intérêt de réduire la quantité d'actifs en circulation est de maintenir la demande supérieure à l'offre et de former un contexte déflationniste, ce qui valorise l'actif à long terme.

Il existe plusieurs mécanismes de destruction. Le plus connu s'opère en transférant des actifs vers un portefeuille verrouillé, également appelé *dead wallet*. Celui-ci est consultable, mais inaccessible, empêchant la récupération des actifs. Ce portefeuille ne possédant pas de *clé privée* (→ 55), les fonds déposés ne sont pas transférables.

La Binance Smart Chain est une des blockchains qui effectue le plus de ***burns*** de ses actifs sur le marché des cryptomonnaies. En effet, pour faire croître le prix du *coin* BNB, la plateforme d'échange a mis en place des mécanismes de destruction automatique avec pour objectif de réduire de moitié l'offre initiale, soit 100 millions de *coins* détruits.

Hachage 27

Le ***hachage*** est une **fonction mathématique qui a pour spécificité de produire une chaîne de caractères d'une taille prédéfinie et fixe** à partir d'une entrée de caractères de longueur aléatoire (également appelé *input*). Ce résultat unique de sortie s'appelle l'empreinte, la signature ou le *hash* dont la particularité est de masquer à la fois le contenu et la longueur du message d'origine.

Une fonction de ***hachage*** doit répondre à **trois conditions essentielles** :

1. **Résistante :** à partir du *hash* final, il est impossible de trouver les caractères d'entrée.
2. **Déterministe :** pour une entrée identique, le *hash* de sortie est toujours le même.
3. **Unique :** pour deux entrées différentes (même très similaires), le *hash* de sortie est complètement différent.

L'une des fonctions les plus connues est le SHA-256 utilisé pour Bitcoin, qui transforme n'importe quel bloc de données en une chaîne de 256 bits (une suite de 256 caractères prenant les valeurs 0 ou 1). Pour des raisons pratiques, cette suite est réduite à 64 caractères grâce au système de numération en base 16 appelé « hexadécimal ». Celui-ci permet de traduire une suite de 4 bits en un caractère prenant une valeur de 0 à 9 ou de A à F. Exemple : la suite « 1010 » est représentée par le caractère « a » dans ce système.

Nous vous proposons ci-après le résultat d'une fonction de ***hachage*** SHA-256 :

Input	***Hash de sortie***
Bonjour	***9172e8eec99f144f72eca9a568759580edadb2cfd154857f07e657569493bc44***
bonjour	***2cb4b1431b84ec15d35ed83bb927e27e8967d75f4bcd9cc4b25c8d879ae23e18***

Nous remarquons que la fonction propose un *hash* de sortie complètement différent lorsque le mot subit une variation même infime (première lettre en majuscule ou non).

Ces fonctions de ***hachage*** sont très utilisées dans le domaine des cryptomonnaies, notamment pour le minage des blocs sur des blockchains fonctionnant en *Proof Of Work* (→ 36) ainsi que pour la création des *clés publiques* (→ 56) et des adresses. Une clé publique est produite par le ***hachage*** de la *clé privée* (→ 55).

Halving 28

Signifiant « réduire de moitié », le ***halving*** est un **événement périodique majeur qui se produit à intervalles réguliers** et concerne différentes cryptomonnaies. Dans cette définition, nous nous attarderons principalement sur le ***halving*** Bitcoin (→3) qui est sans égal en matière d'impacts sur l'écosystème.

L'objectif de cet événement est de contrôler la création cryptomonétaire. Comme prévu par son livre blanc ou *white paper* (→23), ce fonctionnement permettra d'atteindre le maximum des 21 millions de bitcoins autour de l'année 2140.

Le *minage* (→11) est un processus organisé qui permet la sécurisation des réseaux en *Proof Of Work* par des mineurs. Ces derniers contribuent au fonctionnement des réseaux en validant des blocs et sont rétribués en actifs nouvellement créés. Le ***halving*** Bitcoin implique la division de moitié de cette récompense en bitcoins et donc une forte réduction du rythme de la création cryptomonétaire.

Cet événement intervient tous les 210000 blocs validés, soit environ tous les quatre ans puisqu'un bloc est validé approximativement toutes les dix minutes. À la création du bitcoin, la récompense était de 50 BTC, divisée par deux le 28 novembre 2012 à 25 BTC, puis le 9 juillet 2016 à 12,5 BTC pour enfin porter la récompense des mineurs à 6,25 BTC par bloc validé le 11 mai 2020. Le dernier ***halving*** a eu lieu le 20 avril 2024 et a porté la récompense à 3,125 BTC. Ce fonctionnement crée une pression inflationniste sur le prix du bitcoin et contribue historiquement à la hausse du cours du Bitcoin.

29 Hashrate

Signifiant « taux de hachage », le ***hashrate*** est **l'indicateur de puissance de calcul mis à disposition par l'ensemble des mineurs** pour créer un bloc sur une blockchain fonctionnant en *Proof Of Work*.

Exprimé en *hash* par seconde (h/sec), le ***hashrate*** d'un mineur représente sa capacité à chercher le *nonce*, résultat de l'équation mathématique permettant de valider un bloc et d'obtenir la récompense de minage. Plus le nombre de participants au minage d'un bloc est important, plus le taux de hachage est élevé.

Historiquement, le taux de hachage sur Bitcoin est en constante augmentation puisqu'un nombre croissant de mineurs intervient sur le marché. La difficulté de création d'un bloc s'adapte au taux de hachage afin de maintenir constant le temps nécessaire pour valider les données (autour de dix minutes).

Le ***hashrate*** d'une blockchain est donc un gage de sécurité et de confiance puisqu'il prouve la présence d'un nombre important de validateurs sur un réseau, réduisant ainsi les probabilités d'une *attaque des 51 %* (→ 54).

Le taux de hachage est en fluctuation permanente et dépend de différents facteurs tels que l'environnement politique, le coût de l'énergie, la disponibilité des composants électroniques et le cours des actifs.

Layer 30

Signifiant « couche », un ***layer*** désigne **les différents niveaux d'infrastructure d'une blockchain** souvent représentés sous forme pyramidale dont les étages additionnels permettent d'améliorer les fonctionnalités de la structure initiale.

À ce jour, il existe trois niveaux principaux d'infrastructure :

1. ***Layer* 0 :** comparé aux fondations d'un bâtiment, le ***layer*** 0 est un socle commun dont dispose l'ensemble des blockchains incluant les nœuds, les serveurs, les mineurs ou validateurs et Internet permettant les transactions entre les participants du réseau. Chaque ***layer*** 0 dispose de son propre protocole composé de diverses fonction-nalités aidant à résoudre des problèmes de scalabilité, de sécurité ou d'interopérabilité. Polkadot (DOT), Avalanche (AVAX) et Cosmos Hub (ATOM) sont des exemples de ***layer*** 0.
2. ***Layer* 1** : comparé à la structure principale d'un bâtiment, le ***layer*** 1 désigne une blockchain souveraine. Il contient les fonctionnalités élémentaires telles que le mécanisme de consensus, l'historique des blocs, les outils de communication et les applications décentralisées permettant son fonctionnement en autonomie. Les utilisateurs peuvent ainsi réaliser des transactions, créer des *smart contracts* et les déployer. Les ***layers*** 1 prédominants sont Bitcoin et Ethereum ;
3. ***Layer* 2** : cette couche est une réponse au trilemme de la blockchain permettant principalement d'améliorer sa scalabilité. Il bénéficie de la décentralisation ainsi que de la sécurité du ***layer*** 1 et est donc indissociable de ce dernier.

Il peut être comparé à l'extension d'un bâtiment puisqu'il vient se greffer à la structure principale en proposant une amélioration. Le ***layer*** 2 le plus connu est le *Lightning Network* (→31) qui permet d'augmenter la vitesse des transactions sur Bitcoin.

Lightning Network 31

Signifiant « réseau éclair », le ***Lightning Network*** est **une solution technologique au problème de scalabilité auquel Bitcoin fait face**. En effet, le nombre de transactions traitées par seconde est limité : un bloc est miné toutes les dix minutes. Avec une capacité d'approximativement 2 à 3 Mo, un bloc ne peut contenir qu'environ 2500 transactions. En cas de franchissement de cette limite, les transactions sont mises en attente et sont traitées par ordre de priorité selon le montant des commissions offertes, obligeant les utilisateurs à augmenter ces dernières pour obtenir un traitement rapide.

Le concept de ***Lightning Network*** a été présenté pour la première fois en 2015 dans un livre blanc rédigé par Joseph Poon et Thaddeus Dryja. Ces derniers proposaient de mettre en place un réseau décentralisé de canaux de paiement en dehors de la blockchain Bitcoin via une implémentation logicielle du protocole.

Voici comment se déroule le ***Lightning Network*** dans la pratique :

1. Deux individus décident d'ouvrir un canal privé d'échange d'actifs.
2. Ils déposent leurs fonds sur une adresse multisignature commune sur la blockchain.
3. Sur le canal d'échange, chaque compte est crédité du montant déposé sur l'adresse commune.

4. Les individus peuvent ensuite s'échanger leurs actifs quasiment instantanément sur ce canal sans la nécessité de passer par la blockchain.
5. Les soldes des comptes sont calculés à chaque transaction sur le canal privé, mais ne sont pas inscrits sur la chaîne principale.
6. Les individus peuvent décider de fermer le canal pour échanger avec d'autres acteurs. Les informations sur les soldes vont ainsi être mises à jour sur la blockchain et chacun pourra récupérer ses actifs.

Les principaux avantages résident dans la réduction des *fees* (→ 42) (il n'est plus nécessaire de payer les mineurs, car les transactions ne passent pas sur la blockchain), la quasi-instantanéité des transactions (contre dix minutes en moyenne) et la confidentialité des transactions (ces dernières ne sont pas inscrites sur la blockchain, seuls les soldes finaux le seront).

À ce jour, le réseau est toujours en phase de test et comporte plus de 86 500 canaux utilisés par plus de 20 000 nœuds, soit une hausse de la fréquentation de 600 % depuis sa création.

Mécanisme de consensus 32

Également appelé « algorithme de consensus », un ***mécanisme de consensus*** est **l'ensemble de règles qui régit la création de nouveaux blocs** permettant aux utilisateurs de **s'accorder sur l'état du réseau**.

La technologie blockchain fonctionne sur des réseaux de *pair-à-pair* (→ 61). Ainsi, les utilisateurs ne peuvent pas se remettre à une autorité qui détiendrait le pouvoir de décision et de vérification des données. Il est donc nécessaire que ces derniers s'accordent sur un ensemble de règles permettant de confirmer les informations contenues dans les blocs ainsi que leur intégration au sein de la blockchain.

Il existe deux mécanismes universellement utilisés :

1. Le *Proof Of Work* (→ 36) utilisé surtout par la blockchain Bitcoin. Une des règles de cet algorithme prévoit par exemple que chaque première transaction d'un bloc représente la récompense de minage.
2. Le *Proof Of Stake* (→ 35) notamment en place au sein de la blockchain Ethereum. Une règle du mécanisme prévoit par exemple de punir les actions frauduleuses d'un participant en imputant une partie des ethers mis en jeu.

Il n'existe pas de ***mécanisme de consensus*** parfait. Chaque mécanisme tente de trouver un compromis entre trois notions essentielles qui forment le trilemme de la blockchain :

1. **La décentralisation :** assurer que le réseau ne soit pas concentré en quelques acteurs importants qui pourraient avoir un poids sur le marché.
2. **La sécurité :** proposer un réseau fiable et inviolable.
3. **La scalabilité :** établir un réseau efficace permettant des transactions rapides entre les utilisateurs.

Nœud 33

D'un point de vue informatique, un ***nœud*** est **un périphérique physique en mesure de recevoir, stocker et envoyer des informations**. Un ordinateur et un téléphone portable sont des ***nœuds***.

Dans le cadre d'un réseau de *pair-à-pair* (→ 61), les ***nœuds*** sont essentiels, car ils permettent la décentralisation et la sécurisation du réseau en participant au processus de stockage des transactions et à la validation des informations.

Il existe différents types de ***nœuds*** présents sur la blockchain dont nous vous proposons les deux plus courants :

1. **Les *nœuds* légers** : ils ne stockent pas la totalité des échanges réalisés sur la blockchain, mais contrôlent de manière spécifique certaines transactions grâce à une fonctionnalité appelée SPV (*Simplified Payment Verification*). Celle-ci permet de ne conserver que les en-têtes de blocs et donc de limiter le besoin de stockage de données. Les ***nœuds*** légers vont s'appuyer sur les ***nœuds*** complets pour obtenir les informations nécessaires à la validation des transactions.
2. **Les *nœuds* complets** : ils sont les garants des règles de consensus. Ils ont également la capacité de vérifier la totalité des transactions sur la blockchain et détiennent une copie de l'historique de celle-ci.

Il existe différents types de ***nœuds*** complets tels que les ***nœuds*** de minage utilisés pour résoudre des problèmes mathématiques lors de la création de nouveaux blocs sur certaines chaînes de blocs ou bien les ***nœuds*** maîtres (*masternodes* en anglais) utilisés sur des blockchains en *Proof Of Stake* qui nécessitent d'immobiliser des actifs sur le protocole.

34 Oracle

Un ***oracle*** est **une infrastructure permettant de transmettre des données entre le monde *off-chain*** (c'est-à-dire le monde réel observable) **et la blockchain**.

Par conception, les réseaux blockchains sont totalement isolés du monde extérieur et ne peuvent pas interagir avec des données telles que des informations météorologiques, des taux de change et bien d'autres informations essentielles pour le fonctionnement des services proposés sur les plateformes. L'***oracle*** sert donc d'intermédiaire pour transmettre ces données et les traduire d'un réseau à un autre.

Lorsque l'infrastructure transmet des données du monde réel vers la blockchain, on parle d'***oracle*** d'entrée. Celui-ci peut par exemple transmettre les coordonnées GPS d'un avion sur la blockchain qui permet une action spécifique lorsque celui-ci a atterri.

Pour le fonctionnement inverse, on parle d'***oracle*** de sortie, l'infrastructure transmet alors des informations de la blockchain vers le monde externe. On peut imaginer une situation où un utilisateur envoie des fonds pour acheter une marchandise. Une fois l'argent reçu par le *smart contract*, celui-ci permet l'ouverture d'un casier connecté.

Il existe plusieurs types d'***oracles*** dont les deux plus connus sont les suivants :

1. **Les *oracles* logiciels** : ils interagissent avec des sources provenant d'Internet (sites web, base de données en ligne, serveurs indépendants…) et les transmettent directement sur la blockchain. Ces données peuvent être des prix d'actifs numériques, des informations de vol en temps réel ou des résultats de rencontres sportives. Pour éviter des manipulations ou fraudes, l'***oracle*** va généralement utiliser différentes sources pour confirmer les informations reçues.
2. **Les *oracles* matériels** : ces ***oracles*** interagissent avec des sources de données réelles et convertissent des éléments physiques en valeurs numériques analysables par les *smart contracts*. À titre d'exemple, ces ***oracles*** peuvent être utilisés dans la *supply chain* pour suivre le transport de marchandises. À l'aide de capteurs, l'***oracle*** peut indiquer lorsque la marchandise est arrivée à l'endroit spécifié sur le contrat et le transmettre au *smart contract* qui permet le paiement au fournisseur.

35 POS (Proof Of Stake)

Avertissement : nous vous conseillons de lire l'explication du terme de *blockchain* (→ 4) avant de prendre connaissance de cette définition.

Signifiant « preuve d'enjeu », le ***Proof Of Stake*** est **un des mécanismes de consensus les plus utilisés permettant la validation des blocs sur une blockchain**. Notez qu'il sera également possible de trouver d'autres traductions de ce mécanisme : « preuve de participation » ou « preuve d'intérêt ».

Le mécanisme de preuve d'enjeu, contrairement au mécanisme de preuve de travail, ne s'appuie pas sur la puissance de calcul du réseau pour fonctionner, mais sur l'immobilisation d'actifs. Les acteurs participant à la sécurisation du réseau s'appellent des *minters* (pour « batteurs de monnaies »). Ethereum, la deuxième blockchain la plus importante de l'écosystème utilise ce mécanisme.

En pratique, le fonctionnement est le suivant :

1. Chaque acteur qui participe à la sécurisation du réseau immobilise un certain nombre d'actifs. On parle également de mise en séquestre des actifs ou de *staking* (d'où le terme de ***Proof Of Stake***).
2. Le choix du *minter* qui valide un nouveau bloc se fait généralement aléatoirement et proportionnellement au nombre de jetons mis en séquestre. Ainsi, si un *minter* détient 100 000 unités d'un jeton, il a dix fois plus de chances d'être choisi pour la validation du prochain bloc qu'un autre détenteur possédant 10 000 unités, si ni l'un ni l'autre

n'ont pas participé à la loterie précédente.

3. Le *minter* désigné a un temps déterminé pour produire le bloc demandé. S'il ne respecte pas ce délai, un autre *minter* sera désigné.
4. Le *minter* regroupe alors l'ensemble des nouvelles transactions dans un bloc en y intégrant l'identification du bloc précédent. Il signe numériquement pour prouver la propriété de son compte et partage le bloc à l'ensemble des membres du réseau pour vérification. À l'issue de ces opérations, le *minter* reçoit une récompense.
5. Si le *minter* tente de tromper le réseau par la validation de blocs frauduleux, ce dernier recevra des pénalités qui se traduiront par la saisie de tout ou partie des actifs immobilisés (d'où le concept de preuve d'enjeu). Ce mécanisme de pénalités est appelé *shlashing*.

Comparé au mécanisme de preuve de travail, ce mécanisme présente deux avantages majeurs :

1. La faible consommation d'énergie : lorsqu'Ethereum a modifié son mécanisme de consensus passant du POW au ***POS***, le réseau a déclaré que son fonctionnement nécessiterait 99 % d'énergie en moins.
2. Les frais de transaction sont moins élevés.

Deux inconvénients majeurs peuvent aussi être mis en lumière :

1. Le risque de concentration du pouvoir de validation : la majorité des blockchains fonctionnant en ***POS*** détermine semi aléatoirement le validateur selon le nombre d'actifs détenus, les acteurs ayant mis en séquestre le plus d'actifs sont donc privilégiés.
2. La disponibilité des actifs : il est nécessaire de mettre en séquestre des actifs pendant une période prédéfinie souvent assez longue. Les *minters* n'ont donc pas accès à leurs fonds quand ils le souhaitent.

36 POW (Proof Of Work)

Avertissement : nous vous conseillons de lire l'explication du terme de *blockchain* (→ 4) avant de prendre connaissance de cette définition.

Signifiant « preuve de travail », le ***Proof Of Work*** est **un des mécanismes de consensus les plus utilisés permettant la validation des blocs sur une blockchain**.

Ce mécanisme de consensus est utilisé pour faire fonctionner la blockchain la plus importante du marché : Bitcoin.

Pour résumer simplement ce mécanisme en quatre points essentiels :

1. Chaque bloc présent dans la blockchain possède un *hash* unique, c'est-à-dire une identification spécifique. Le *hash* est le résultat d'une fonction de *hachage* (→ 27) qui transforme des données contenues dans un bloc en une sortie de caractères.
2. Pour valider un bloc, les mineurs doivent résoudre une équation mathématique. Cette équation consiste à trouver une chaîne de caractères qui, ajoutée au *hash* du bloc précédent, permettra d'obtenir un résultat spécifique (exemple : un *hash* commençant par 5 zéros).
3. La fonction de hachage est une fonction que l'on appelle *preimage resistant*, c'est-à-dire qu'il est impossible de définir les termes de l'équation à partir de son résultat. Ainsi, la seule manière de faire coïncider son résultat avec

les spécifications demandées est de tester une à une des combinaisons aléatoires. Les mineurs utilisent la puissance de calcul de leurs ordinateurs pour tester des milliards de possibilités jusqu'à trouver le résultat. C'est pour cette raison que l'on appelle cette méthode la « preuve de travail ».

4. Lorsque le mineur a trouvé la solution à l'équation, cela forme le *hash* final du nouveau bloc qui sera intégré au bloc suivant pour reproduire la même opération.

Cette méthode de consensus offre donc une sécurité importante pour l'ensemble du réseau ainsi qu'une grande liberté pour les mineurs qui peuvent commencer et arrêter de contribuer à la sécurisation du réseau comme ils le souhaitent. Le fonctionnement du ***POW*** prévoit qu'à mesure que les réseaux blockchains sont rejoints par des mineurs, la difficulté augmente afin de garantir la sécurité sur l'ensemble du réseau.

Le défaut majeur de cette méthode réside dans son besoin en énergie pour faire fonctionner les appareils de minage induisant un coût important sur le réseau. Ces dépenses énergétiques ont évidemment un impact écologique. Selon une étude menée par Selectra, la consommation d'énergie annuelle du Bitcoin est plus importante que celle de 199 des 230 pays du monde.

37 Solidity

Solidity est un **langage de programmation conçu pour l'écriture de *smart contracts*** permettant la création d'applications décentralisées principalement exécutées sur l'Ethereum Virtual Machine (EVM).

Créé par le cofondateur d'Ethereum, Gavin Wood, en 2014, ce langage de programmation comporte des similitudes avec JavaScript, Python et C++, ce qui permet à un développeur connaissant ces derniers d'adopter facilement ce mode d'écriture.

Voici un exemple de ce langage de programmation d'un *smart contract* intitulé « Hello World » :

```
//SPDX-License-Identifier :
MITpragma solidity ^0.8.24;
contract HelloWorld
{string public greet = « Hello World ! » ;}
```

Ce *smart contract* (→ 17) est un exemple utilisé à des fins pédagogiques pour démontrer les bases de la programmation en ***Solidity***. Grâce à ce code, il est possible de consulter un message de salutation sous forme de chaîne de caractères sur la blockchain Ethereum.

Chapitre 3

Des mots pour mettre en pratique

Votre lecture vous a permis jusqu'à présent de comprendre l'essentiel du fonctionnement des technologies sous-jacentes aux cryptoactifs, mais certaines notions ont pu vous sembler parfois très théoriques. Dans ce chapitre, nous vous présentons des applications concrètes et fonctionnelles dont de nombreux individus ne peuvent désormais plus se passer et qui feront peut-être partie de votre quotidien dans le futur.

38 API (Application Programming Interface)

Signifiant « interface de programmation pour application », un ***API*** est une **liaison permettant à deux applications de communiquer entre elles**.

Cette interface permet à un programmeur d'utiliser la fonctionnalité d'une application préexistante pour l'ajouter à la sienne, lui évitant ainsi le développement d'une nouvelle. Pour un programmeur, l'utilisation d'une ***API*** est un véritable gain de temps, mais cela nécessite d'avoir une ***API*** *key*, clé permettant d'acquérir les droits d'utilisation. Cette sécurité assure le transfert des fonctionnalités en assurant l'origine de celles-ci.

DAO (Decentralized Autonomous Organization) 39

Signifiant « organisation autonome décentralisée », une ***DAO*** est **une entité dont le fonctionnement n'est pas régi par un organe central, mais par des règles de gouvernance inscrites dans un *smart contract*** (→ 17).

La gestion de cette organisation et les prises de décision se font de manière collective et démocratique autour d'une communauté : chaque détenteur d'un *token* (→ 19) de la structure possède un droit de vote proportionnel au nombre de jetons détenus.

L'exemple le plus célèbre de ce type d'organisation est le projet The ***DAO*** lancé en 2016 sur Ethereum. Cette organisation fonctionnait comme un fonds de capital-risque : des projets lui étaient soumis et les copropriétaires prenaient les décisions d'investissement. Le projet prit de l'ampleur et près de 150 millions de dollars furent collectés par l'organisation. Néanmoins, le 17 juin 2016, un pirate informatique trouva une faille dans le code du projet The ***DAO*** et détourna des millions de dollars, faisant perdre beaucoup d'argent à un grand nombre d'investisseurs. Cette attaque fut à l'origine de la division de la communauté Ethereum et du *fork* (→ 43) le plus connu de l'histoire des cryptomonnaies.

40 Dapp (Decentralized Application)

Signifiant « application décentralisée », une ***Dapp*** est **une application qui fonctionne sans autorité centrale grâce à la technologie blockchain** et qui offre une expérience utilisateur similaire aux applications les plus connues.

La décentralisation de ces applications est régie par la combinaison d'une interface utilisateur interactive et d'un *smart contract* (→ 17) stocké sur la blockchain. Le code de l'application est libre d'accès et les données récoltées par l'utilisation de l'application sont stockées sur une blockchain. Cette technologie étant onéreuse, un actif est généralement utilisé afin de permettre d'interagir avec la ***Dapp***.

L'usage de la technologie blockchain permet un fonctionnement continu de l'application qui ne sera pas sensible à une panne de serveur par exemple. Son utilisation est pseudonyme, ce qui accentue la confidentialité de l'utilisateur.

Explorateur Blockchain 41

L'***explorateur blockchain*** est **un site web comparable à un navigateur permettant d'effectuer des recherches sur les blockchains** afin de consulter toutes les informations liées aux transactions.

Concrètement, l'explorateur est une interface entre l'homme et la blockchain et permet d'extraire les données validées et enregistrées dans les blocs depuis sa création. Ces données sont particulièrement fiables puisque les blockchains sont immuables et infalsifiables. Chaque blockchain publique dispose d'au moins une interface pour la consulter accessible à tout individu, les blockchains privées étant consultables uniquement par les utilisateurs autorisés.

Vous pouvez utiliser des sites web comme *blockchain.com* ou *blockchair.com* pour consulter toutes les informations de différentes blockchains depuis leur création. Vous pourrez par exemple retrouver l'information sur la plus célèbre transaction effectuée en bitcoins, réalisée le 22 mai 2010 et enregistrée sur le bloc 57 043 : l'achat de deux pizzas contre 10 000 BTC. Ce jour est désormais appelé le *pizza day*.

42 Fees

Signifiant « frais », les ***fees*** représentent **une commission qu'un utilisateur doit acquitter lorsqu'il utilise des services sur la blockchain**. Ces frais sont également appelés « frais de réseau », « frais de transaction » ou encore « frais de *gas* ».

Les ***fees*** sont payés par les utilisateurs et servent à rétribuer les acteurs qui traitent les transactions et qui contribuent à la sécurité du réseau.

Les ***fees*** sont déterminés par plusieurs facteurs. Tout d'abord, la complexité des transactions et la taille des données : plus une transaction demande de travail aux validateurs, plus le coût est élevé. Le troisième facteur dépend de la congestion du réseau : selon le nombre d'utilisateurs souhaitant réaliser une transaction à un instant donné, le prix est ajusté. Par exemple, il n'est pas étonnant de voir des frais dix à vingt fois plus importants en pleine journée que dans la nuit. Dans certains cas, il est même possible qu'un coût de transaction soit plus élevé que la transaction elle-même.

En se basant sur ce principe d'offre et de demande, un utilisateur qui souhaite réaliser une transaction très rapidement, peut proposer des frais plus importants afin d'encourager les validateurs à traiter sa demande en priorité.

Le terme de ***fees*** peut également être utilisé par les plateformes d'échanges centralisées tels que Binance ou Kraken, mais les ***fees*** s'apparentent cette fois simplement à des frais d'opération, similaires aux frais des institutions financières traditionnelles (même s'ils restent moins élevés).

Fork 43

Signifiant « fourchette », un ***fork*** désigne **la division d'une blockchain en plusieurs branches distinctes**. Le terme de ***fork*** peut également être traduit par « embranchement ».

Il existe deux grands types de ***forks*** :

1. **Les *hard forks* :** signifiant « embranchements durs », les *hard* ***forks*** modifient profondément la blockchain et sont très souvent non rétrocompatibles (c'est-à-dire que les nœuds qui ne sont pas à jour ne peuvent plus interagir avec la blockchain). Ces derniers peuvent être soit le fruit d'un consensus, cela signifie que les modifications sont acceptées par la grande majorité de la communauté et que seule la nouvelle chaîne intégrant les améliorations perdure. Les *hard* ***forks*** peuvent également être le fruit d'un contentieux, cela signifie que la communauté est en désaccord sur les nouvelles règles à adopter. Si chacune des deux communautés est suffisamment importante, deux chaînes coexistent portant chacune des protocoles et des fonctionnements différents.

   Le *hard* ***fork*** non consensuel le plus connu fait suite au piratage de The DAO en 2016 sur Ethereum qui a fait perdre des millions d'euros aux utilisateurs. La communauté s'est alors divisée en deux : certains souhaitaient modifier le bloc piraté et rendre l'argent aux utilisateurs et d'autres attachés au concept d'immuabilité des blockchains ne voulaient pas interférer. Ce désaccord a donné lieu à deux chaînes distinctes : Ethereum qui a été modifiée et Ethereum Classic où aucun bloc n'a été modifié.

2. **Les *softs forks* :** signifiant « embranchements souples », ils interviennent lorsque les modifications du protocole sont plus légères et rétrocompatibles. C'est une sorte de « mise à jour » du réseau. Dans ces cas-là, les anciens nœuds restent connectés au réseau et intègrent les nouveaux blocs comme valides. Pour qu'un *soft* ***fork*** soit accepté, il faut qu'il obtienne une opinion favorable de la part d'au moins 51 % des validateurs. Un des exemples les plus célèbres de *soft* ***fork*** est la mise à jour du protocole Bitcoin appelé SegWit (pour *Segregated Witness* que l'on peut traduire par « témoin séparé ») qui visait à optimiser et augmenter la capacité de Bitcoin à traiter les transactions.

Régulièrement, de nombreux ***forks*** anodins que nous appelons « ***forks*** de circonstance » interviennent sur les blockchains en *Proof Of Work* (→ 36). Ces ***forks*** surviennent lorsque deux acteurs valident en même temps des blocs différents. Dans ce cas, deux embranchements distincts apparaissent. Les blockchains ont un protocole simple qui permet de résoudre ce conflit : la chaîne la plus longue est conservée. Ainsi, lorsque d'autres blocs sont ajoutés à la suite de l'une ou l'autre des sorties, la blockchain en conserve automatiquement une et retrouve son fonctionnement naturel sur une seule chaîne.

Gas 44

Signifiant « gaz » ou « essence », le ***gas*** est **un système permettant d'organiser les frais de transactions pour tous les acteurs de la blockchain Ethereum**. Par extension, ce concept est utilisé pour d'autres blockchains se servant du même fonctionnement.

Le ***gas*** assure la fonction d'intermédiaire entre un utilisateur qui réalise une opération sur la blockchain et un validateur qui va enregistrer et intégrer ses transactions sur celle-ci.

Lorsque vous effectuez une transaction sur la blockchain, vous allez rencontrer trois notions importantes :

1. **Le *gas price*** : il s'agit du prix auquel le ***gas*** est acheté. Celui-ci est calculé en fonction du marché, mais il est possible de l'ajuster. En effet, acheter un ***gas*** à un prix plus important encourage les validateurs à traiter votre transaction en priorité, car la récompense associée est plus importante. À l'inverse, l'acheter à un prix inférieur peut faire économiser des frais si l'opération n'est pas urgente.
2. **Le *gas limit*** : il s'agit de la quantité maximale de ***gas*** que l'utilisateur est prêt à dépenser. Lorsque les transactions et les contrats sont exécutés sur la blockchain, ils utilisent du ***gas***. Lorsqu'un contrat n'a plus de ***gas***, il cesse de fonctionner.
3. **Le *gas cost*** : chaque opération sur la blockchain a un coût déterminé en ***gas*** selon la complexité de celle-ci. Ainsi, l'utilisateur est prévenu en amont de l'opération du nombre d'unités de ***gas*** nécessaire pour réaliser sa transaction.

Ainsi, les frais pour une opération sont calculés en multipliant le coût du ***gas*** par le prix d'achat de celui-ci.

Un des intérêts majeurs de ce fonctionnement est de limiter les comportements visant à congestionner le réseau. Si un utilisateur au comportement malveillant souhaitait ralentir le réseau en réalisant des milliers de transactions, il devrait payer des frais pour chaque transaction. Le coût total de l'opération décourage ce type d'actions.

ICO (Initial Coin Offering)

45

Signifiant « offre initiale de jetons », une ***ICO*** est **une opération de levée de fonds dans l'écosystème des cryptomonnaies**. Cette opération est relativement similaire à celle de l'*Initial Public Offering* (→48) dans le monde de la finance traditionnelle.

Le fonctionnement est assez simple : une organisation qui souhaite lever des fonds pour financer un projet va émettre sur une plateforme des jetons que les investisseurs pourront acheter. Pour encourager l'achat, des contreparties à la détention de ses jetons sont proposées. L'argent récolté par la vente des jetons sera utilisé par l'organisme pour développer son projet.

Ces contreparties peuvent être très différentes et sont généralement un droit d'usage du produit ou de service. Évidemment, une partie des investisseurs est également intéressée par l'aspect spéculatif de ces opérations et achète donc ces jetons dans l'objectif de les revendre à un prix plus élevé.

Parmi les ***ICO*** emblématiques de l'écosystème des cryptomonnaies, nous pensons évidemment à l'***ICO*** d'Ethereum en 2014, deuxième cryptomonnaie la plus importante de l'écosystème qui avait permis de lever près de 20 millions de dollars. La plus importante ***ICO*** à ce jour est détenue par le projet EOS qui avait réussi à lever 4 milliards de dollars en 2018.

46 IDO (Initial DEX Offering)

Signifiant « offre initiale de jetons par une plateforme décentralisée », **une *IDO* est une levée de fonds organisée sur une plateforme décentralisée** également appelée DEX pour *Decentralized Exchange*. Son équivalent centralisé est l'*IEO* (→ 47).

Une organisation qui souhaite lever des fonds propose des jetons sur une plateforme d'échange décentralisée. Les fonds récoltés servent à financer le projet et les investisseurs détenant des jetons obtiennent des contreparties soit capitalistiques soit utilitaires.

Le fonctionnement d'une ***IDO*** est bien plus souple et moins contraignant d'un point de vue juridique, les investisseurs restent anonymes et n'ont pas d'obligation de se soumettre à un *KYC* (→ 58). L'investissement est donc plus risqué que pour une IEO puisqu'aucune régulation ni analyse du projet n'est faite en amont.

Une des plateformes spécialisées dans les ***IDO*** et les plus connues de l'écosystème est Polkastarter.

IEO (Initial Exchange Offering) 47

Signifiant « offre initiale de jetons par une plateforme centralisée », une ***IEO*** est **une levée de fonds qui s'opère sur une plateforme d'échange centralisée également appelée CEX pour Centralized Exchange**, contrairement à l'*ICO* (→ 45) qui se réalise directement entre l'entreprise et les investisseurs.

Tout comme l'ICO, une entité va proposer à la vente des jetons afin de financer son projet. Pour cela, elle va passer par une plateforme d'échange réglementée qui va soumettre le projet à tous ses utilisateurs.

Ce fonctionnement comporte plusieurs intérêts pour les trois parties :

1. **Pour les investisseurs** : investir via une ***IEO*** s'avère plus simple et accessible même aux investisseurs débutants par comparaison avec l'ICO qui demande une plus grande maîtrise du fonctionnement de la blockchain et des *smart contracts*. De plus, le projet étant analysé et sélectionné par une plateforme, les projets sont plus dignes de confiance.
2. **Pour les entreprises** : l'intérêt de passer par une ***IEO*** réside principalement dans la visibilité que la plateforme offre. En effet, lorsqu'un projet est validé, il sera proposé sur la plateforme à l'ensemble de sa base d'utilisateurs permettant à l'entité de se faire connaître plus largement que dans le cas d'une ICO où la communication ne dé-

pend que des porteurs du projet. L'autre intérêt se situe sur la simplicité juridique : passer par une plateforme évite à l'entreprise de réaliser un protocole de vérification d'identité contraignant, celui-ci étant réalisé par la plateforme à l'inscription.

3. **Pour les plateformes :** proposer une ***IEO*** possède un double intérêt. Dans un premier temps, financier : les plateformes prennent des frais pour que l'on puisse utiliser ses services. L'autre avantage réside dans l'image de la plateforme, proposer des ***IEO*** permet aux plateformes de développer leur nombre d'utilisateurs.

La plateforme la plus importante qui propose ce type de service est Binance Launchpad.

IPO (Initial Public Offering)

48

Signifiant « introduction en Bourse », une ***IPO*** est un **processus par lequel une entreprise va émettre des actions pour la première fois sur le marché public** et donc être cotée en Bourse. La détention de ces actions va offrir aux investisseurs des droits politiques (vote) et financiers (partage des dividendes).

Ce processus permet aux entreprises de lever des fonds pour permettre le développement de leurs projets. À cet égard, cette opération est assez similaire à celle du *STO* (→ 52) dans l'écosystème des cryptomonnaies.

Pour réaliser cette opération, l'entité va devoir s'engager dans un processus réglementaire et juridique long où un audit complet de la structure sera réalisé avant de pouvoir envisager une ***IPO***. Une fois cotée en Bourse, la société devra répondre à des exigences réglementaires et d'informations : communication des bilans, des comptes de résultat à des intervalles réguliers.

Il existe plusieurs procédures pour faire une introduction en Bourse, parmi lesquelles les plus connues historiquement sont l'OPO et l'OPF :

1. **L'OPO (offre à prix ouvert)** : il s'agit de la procédure la plus courante, l'entreprise propose ses actions à la vente dans une fourchette de prix donné. Le prix et les quantités finals sont déterminés en fonction de la demande des investisseurs.

2. **L'OPF (offre à prix ferme)** : l'entreprise et un établissement financier spécialisé définissent en amont de l'introduction en Bourse le nombre d'actions et le prix de vente unitaire. La quantité finale est déterminée selon la demande des investisseurs.

Une ***IPO*** est donc une procédure complexe qui peut prendre plusieurs mois et qui est particulièrement coûteuse. On estime que le coût d'une introduction en Bourse se situe entre 5 à 10 % du montant des fonds levés.

La plus importante introduction en Bourse de l'histoire s'est déroulée en 2019, il s'agissait de la société pétrolière saoudienne Saudi Aramco qui a permis de lever 29,4 milliards de dollars, détrônant ainsi le précédent record détenu par le géant chinois Alibaba qui avait levé 25 milliards de dollars en 2014.

Launchpad 49

Signifiant « rampe de lancement », le ***launchpad*** est **le terme générique désignant pour un projet ou une entreprise l'une des options pour lever des fonds** en vue de son développement.

Il existe différents types de ***launchpad*** tels que les *IDO* (→ 46) et les *IEO* (→ 47) qui se réalisent sur des plateformes d'échange décentralisées ou centralisées.

Pour participer à ces offres de lancement, l'investisseur doit respecter certaines conditions fixées par les plateformes d'échange dont la majorité exige la détention d'une certaine quantité de *coins* (→ 5) de la plateforme ainsi que le *staking* (→ 51) de ces derniers.

Un certain nombre d'incubateurs de projets de l'écosystème des cryptomonnaies proposent ce type d'investissement. Parmi les incubateurs plus populaires, il existe le Binance Launchpool, Polkastarter, ou encore Duckstarter.

50 Lending

Signifiant « prêt », le ***lending*** permet à un détenteur de liquidités de devenir **prêteur en mettant à disposition son capital sur une plateforme contre des intérêts**.

Le ***lending*** est une stratégie qui peut être mise en place par un individu pratiquant le *holding* (→ 96). Celui-ci se constituant habituellement un portefeuille d'actifs avec un objectif de revente à long terme, peut ainsi diversifier ses sources de revenus avec cette stratégie. Alternative à la mise en sommeil des actifs sur un portefeuille, le prêteur peut ainsi accroître la quantité de jetons détenus et générer un rendement complémentaire en mettant ces derniers à disposition d'un pool de *liquidité* (→ 75) par exemple.

Selon l'offre et la demande de l'actif ainsi que la durée du prêt, le rendement annuel proposé au fournisseur de liquidité varie généralement de quelques pour cent et peut atteindre un rendement annuel à deux chiffres. L'inconvénient majeur de ce type de placement est le blocage des liquidités sur une durée définie, empêchant ainsi l'investisseur de vendre ses actifs à l'instant voulu. Ce fonctionnement est également appelé *vesting*.

En pratique, le ***lending*** fonctionne de la manière suivante :

1. Le prêteur dépose dans un pool de liquidité ses actifs. La rémunération de chaque actif dépend de l'offre et de la demande et évolue selon la durée du prêt.
2. Un utilisateur souhaitant réaliser un emprunt doit déposer sur une plateforme spécialisée des actifs pour pouvoir en

emprunter d'autres. Cette somme, également appelée « collatéral », est mise en séquestre et permet à la plateforme de se prémunir contre le non-remboursement de ses clients.

3. L'emprunteur peut ainsi obtenir des actifs provenant du pool de liquidité. Pour ne prendre aucun risque, notamment à cause de la forte volatilité du marché, la plateforme permet aux utilisateurs d'emprunter une somme systématiquement inférieure au séquestre déposé.
4. Lorsque l'emprunteur restitue le prêt avec les intérêts sur la plateforme, son séquestre lui est restitué directement grâce à un *smart contract* (→ 17).
5. Si l'emprunteur ne rembourse pas le prêt ou qu'à cause de la volatilité du marché, la valeur globale des actifs sous séquestre diminue en dessous d'un seuil prédéfini (proche de la somme empruntée), le collatéral est vendu et le prêteur remboursé.

51 Staking

Signifiant « jalonnement », le ***staking*** est un **processus qui permet entre autres de sécuriser les blockchains en *Proof Of Stake*** en verrouillant une quantité d'actifs et en obtenant des récompenses en contrepartie.

En pratique :

1. Un individu immobilise des actifs dans un *smart contract* (→ 17), on dit qu'il « met en jeu » ses actifs, d'où le mécanisme de consensus de *Proof Of Stake* ou « *preuve d'enjeu* ».
2. L'utilisateur devient alors un validateur (ou *minter*) qui est sélectionné aléatoirement par l'algorithme. Lorsqu'il est sélectionné, le *minter* doit valider le bloc et l'intégrer à la blockchain.
3. Si le validateur tente de tromper le réseau en validant des blocs frauduleux, celui-ci sera pénalisé par la perte de tout ou partie des actifs mis en jeu.
4. En contrepartie de cet engagement, le *minter* reçoit une rémunération (en actifs identiques à ceux verrouillés) qui est définie selon la quantité d'actifs mis en jeu et la durée d'engagement. Contrairement aux réseaux en *Proof Of Work*, ces récompenses sont régulières et ne dépendent pas de la validation d'un bloc, mais bien de la mise en jeu d'actifs.
5. La mise en jeu des actifs est possible selon deux modalités. Soit un engagement flexible permettant à l'utilisateur de retirer à tout moment ses actifs (impliquant une rémunération moins intéressante), soit un engagement ferme

sur une durée durant laquelle il ne sera pas possible de récupérer ses actifs.

6. Les intérêts perçus sont indiqués sous forme d'APY, abréviation de *Annual Percentage Yield* signifiant « pourcentage de rendement annuel ».

Le ***staking*** est la pierre angulaire du mécanisme de consensus du *Proof Of Stake* et offre une sécurité importante sans l'inconvénient de la consommation excessive d'énergie inhérente au mécanisme du *Proof Of Work*.

52 STO (Security Token Offering)

Signifiant « offre de jetons-titres », une ***STO*** est une **opération de levée de fonds dans l'écosystème des cryptomonnaies s'appuyant sur des jetons financiers**. Cela permet à une organisation de financer un projet en proposant des *tokens* à la vente auprès d'investisseurs sur une blockchain.

Cette levée de fonds se distingue des autres types tels que l'*ICO* (→ 45), l'*IDO* (→ 46) ou l'*IEO* (→ 47) par le fait que les jetons proposés à la vente sont spécifiques : il s'agit de *security tokens* ou « jetons-titres » qui sont considérés par les autorités financières comme des valeurs mobilières et font donc l'objet d'une réglementation particulière. En effet, ces derniers offrent des droits financiers et/ou politiques au même titre qu'une action ou une obligation, les distinguant des autres types de *tokens*. Les ***STO*** se réalisent donc sur des plateformes de délivrance soumises à une régulation stricte.

Il existe deux principaux types de *tokens* émis lors d'une ***STO*** :

1. **Les *Equity Tokens*** : ces jetons sont semblables à des actions.
2. **Les *Debt Tokens*** : ces jetons sont semblables à des obligations.

Les ***STO*** sont donc réglementairement beaucoup plus complexes à mettre en place pour une entité que les autres formes de levées de fonds, mais offrent en contrepartie la

possibilité d'attirer beaucoup plus d'investisseurs avec une confiance accrue et un intérêt pécuniaire plus fort.

Les ***STO*** facilitent considérablement l'accès pour les entreprises à ce type de financement que son équivalent dans la finance traditionnelle, l'*IPO* (→ 48) qui est principalement réservée aux très grandes entreprises, car très coûteuse.

Chapitre 4

Assurer la sécurité de ses actifs et de ses données

Utiliser les cryptoactifs et les services financiers qui y sont associés peut parfois s'avérer risqué, surtout lorsque l'on débute dans ce domaine. L'absence de tiers de confiance et la décentralisation obligent les individus à être alertes et à connaître les règles essentielles de sécurisation de leurs actifs et leurs données. Ce chapitre compile treize mots autour de la sécurité et des risques associés à cet écosystème.

53 2FA (Two-Factor Authentificator)

Signifiant « authentification à deux facteurs », le ***2FA*** est une **méthode de sécurisation en deux étapes** des comptes utilisateurs. Il permet d'augmenter le niveau de sécurité d'un compte en ajoutant à une première identification traditionnelle, un second moyen d'authentification.

La première étape, appelée « **facteur de connaissance** », est fixe : composée d'un identifiant et d'un mot de passe. La deuxième, appelée « **facteur de possession** », est générée aléatoirement à intervalles réguliers par une application mobile ou l'envoi d'un code par SMS.

Un **facteur d'inhérence** remplace parfois le facteur de possession. Ce moyen consiste à utiliser une caractéristique biométrique telle que la reconnaissance faciale, vocale ou l'empreinte digitale.

Cette authentification forte permet d'éviter la connexion frauduleuse à distance d'un individu qui aurait réussi à récupérer le facteur de connaissance de l'utilisateur.

Attaque des 51 % 54

Également appelée « Attaque à la majorité », ***l'attaque des 51 %*** est une **tentative de corruption d'une blockchain** fonctionnant en *Proof Of Work* (→ 36) par la possession d'au moins 51 % du taux de hachage ou *hashrate* (→ 29) en anglais.

Grâce à une telle puissance de calcul, l'attaquant pourrait réaliser une double dépense, voire imposer son consensus à l'ensemble du réseau comme suit :

1. L'attaquant crée une bifurcation de la chaîne, également appelée *fork* (→ 43), sur laquelle il valide seul les blocs grâce à sa puissance de calcul. Deux chaînes de blocs sont donc développées en simultané, une par les mineurs honnêtes et l'autre par le mineur malveillant.
2. Celui-ci réalise une transaction sur la chaîne honnête.
3. Le mineur malhonnête vérifie plus rapidement les blocs sur la chaîne malveillante que sur la chaîne honnête afin de créer une blockchain plus longue.
4. Il diffuse ensuite la chaîne piratée au réseau, obligeant tous les mineurs à travailler sur sa version puisque la règle de gouvernance leur impose de miner sur la plus longue.
5. La blockchain honnête devient donc invalide et l'ensemble de ces transactions sont annulées et remboursées, y compris celle réalisée par l'attaquant.
6. Le protagoniste qui s'est vu annuler sa dépense initiale sur la chaîne honnête pourra réutiliser ses fonds sur la nouvelle chaîne, on parlera alors de « double dépense ».

Néanmoins, **posséder 51 % du *hashrate* ne garantit pas de pouvoir corrompre la blockchain**, rendant ainsi le résultat de cette attaque incertain. En effet, cela ne garantit qu'une probabilité d'environ une sur deux d'être le mineur qui trouvera la solution à l'équation permettant de valider le bloc. Pour augmenter sa probabilité de résultat, l'attaquant devra donc augmenter sa puissance de calcul et détenir bien plus que 51 % du *hashrate*.

Ce type d'attaque est en réalité très peu probable puisqu'elle impose des coûts astronomiques en matériels, infrastructures et énergie. De plus, même si un acteur malveillant se trouvait en position de corrompre une blockchain, réussir une telle attaque impacterait fortement la confiance des utilisateurs faisant ainsi chuter la valeur du butin de l'attaquant.

À ce jour, le coût d'opportunité d'une ***attaque à 51 %*** sur la blockchain Bitcoin est estimé à environ 20 milliards d'euros et constitue un véritable exploit pour ce qui est de l'approvisionnement en pièces et matières premières. Des actions malhonnêtes de ce type sont donc découragées, car moins rentables et moins durables que de participer à la sécurisation du réseau afin de percevoir les récompenses de bloc.

Clé privée 55

Une ***clé privée*** est un **élément essentiel de sécurisation des cryptomonnaies** se présentant sous la forme d'une chaîne alphanumérique qui possède un double intérêt : elle permet d'accéder aux actifs et de pouvoir les transférer sur d'autres adresses.

La ***clé privée*** est liée au concept de *cryptographie* (→ 57) asymétrique. Celle-ci sert principalement à déchiffrer les éléments que les autres utilisateurs transmettent à l'aide de la clé publique qui lui est associée. Sur une blockchain, les individus utilisent également leur ***clé privée*** afin de «signer leurs transactions» et donc de garantir la provenance de celle-ci.

Ce qu'il est important de comprendre, c'est que lorsqu'un individu détient des cryptoactifs, il ne les possède pas directement. En réalité, il possède la ***clé privée***, c'est-à-dire la clé permettant d'accéder à l'adresse détenant les actifs. Pour imager ce fonctionnement, on peut prendre l'exemple d'un coffre-fort : l'individu détient la clé pour ouvrir le coffre-fort, mais ne se déplace jamais avec celui-ci. Cela signifie que si la clé est perdue ou volée, n'importe quel individu peut s'emparer des actifs.

Une précision concernant les plateformes d'échange grand public telles que Coinbase ou Kraken. Lorsque vous créez un compte auprès de ces fournisseurs de services financiers, vous ne possédez pas de ***clé privée***, ce sont les plateformes qui conservent et sécurisent vos actifs à votre place. Dans ces cas, on parle de comptes *custodial* par opposition aux comptes *non custodial* où vous détenez personnellement vos clés privées.

56 Clé publique

Une ***clé publique*** est une adresse publique se présentant sous la forme d'une chaîne alphanumérique qui permet de recevoir des actifs numériques. Ainsi, toute personne connaissant votre ***clé publique*** peut vous envoyer des cryptomonnaies et consulter vos transactions. En revanche, pour revendiquer l'usage de ces fonds, il est nécessaire d'avoir la clé privée correspondante.

Une ***clé publique*** est générée à partir d'une clé privée. En *cryptographie* (→ 57), votre ***clé publique*** sert à chiffrer des messages que seul le détenteur de la clé privée associée peut déchiffrer. Elle sert également à vérifier l'authenticité et la provenance d'une transaction sur la blockchain.

Pour mieux comprendre le fonctionnement des clés privées et publiques, une image est souvent utilisée : celle de la boîte aux lettres. Une ***clé publique***, c'est l'adresse de votre boîte aux lettres, celle qui permet à n'importe quel utilisateur de vous trouver et de vous déposer des enveloppes. En revanche, pour récupérer votre courrier, vous devez posséder la clé d'ouverture de la boîte aux lettres, à savoir la clé privée.

Cryptographie 57

La ***cryptographie* est l'étude des techniques et mécanismes visant à chiffrer des messages pour les protéger**. Elle constitue une des deux branches d'une science appelée « cryptologie », étymologiquement « science du secret ». L'autre branche de la cryptologie est la cryptanalyse, qui est l'étude de déchiffrement de messages protégés.

La ***cryptographie*** poursuit quatre objectifs principaux :

1. **La confidentialité** : assurer que les informations ne peuvent être déchiffrées que par les utilisateurs autorisés.
2. **L'authentification** : garantir l'identification de l'émetteur du message.
3. **L'intégrité** : garantir que les informations n'ont pas été modifiées après leur envoi.
4. **La non-répudiation** : empêcher un émetteur de nier l'envoi de données.

Pour chiffrer un message, on utilise un *algorithme de chiffrement* qui s'appuie sur des fonctions mathématiques complexes et une ou plusieurs clés. Il existe deux grands types d'algorithmes de chiffrement :

1. **Symétriques** : une même clé cryptographique est utilisée pour chiffrer et déchiffrer les messages. Ainsi, l'ensemble des acteurs du réseau doivent posséder cette clé pour échanger des informations.
2. **Asymétriques** : deux clés différentes sont utilisées, l'une pour chiffrer et l'autre pour déchiffrer les messages. Ces deux clés sont mathématiquement liées, la clé pri-

vée permettant de générer une clé publique, mais pas réciproquement.

La ***cryptographie*** asymétrique est essentielle dans le fonctionnement des cryptomonnaies, notamment pour la signature des transactions. Elle permet de faire fonctionner le réseau de manière *trustless* (→64), c'est-à-dire sans avoir besoin de faire confiance aux acteurs du réseau ou à un organe tiers.

KYC (Know Your Customer)

58

Signifiant «connaître votre client», le ***KYC*** désigne **le processus de vérification de l'identité des clients** souhaitant utiliser des services financiers.

Dans la finance traditionnelle, ce processus de vérification de l'identité est obligatoire pour tous les fournisseurs de services financiers. Dans l'univers des *cryptomonnaies* (→ 6), le ***KYC*** est également obligatoire pour un certain nombre d'entités régulées, notamment les plateformes d'échange centralisées telles que Binance ou Kraken. À l'inverse, les services entièrement décentralisés tels que les DEX ne sont pas régulés et ne demandent donc pas ce type de vérification.

Le ***KYC*** en cryptomonnaie poursuit le même objectif que celui utilisé par les établissements de la finance traditionnelle : il permet de s'assurer de l'identité du client et de ses antécédents et donc de limiter les activités de blanchiment d'argent ou de financement du terrorisme.

Généralement, les fournisseurs de services financiers demandent un justificatif de domicile ainsi qu'une pièce d'identité. Parfois, cette vérification est complétée par un processus de comparaison faciale : une photo de l'utilisateur, muni de sa pièce d'identité, doit être réalisée directement via l'application ou le site Internet du fournisseur.

59 Ledger

Ledger est une société française basée à Vierzon qui **produit et commercialise un portefeuille physique ou hardware *wallet*** (→ 21). Celui-ci se présente sous l'apparence d'une clé USB permettant de sécuriser les cryptoactifs.

Contrairement aux idées reçues, ce portefeuille permet non pas de stocker directement les actifs des individus, mais bien de conserver les *clés privées* (→ 55) des utilisateurs attestant de leur détention.

La société ***Ledger*** est fondée en 2014 par plusieurs entrepreneurs, dont Éric Larchevêque, et emploie près de 800 personnes à ce jour. Elle est la première entreprise de l'écosystème des cryptomonnaies à obtenir la certification de sécurité de premier niveau (CSPN) qui atteste que les systèmes de sécurité de ses produits sont conformes aux normes établies par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). En février 2024, elle se classe dix-huitième au rang des licornes françaises (startup des nouvelles technologies valorisées au minimum à 1 milliard de dollars).

Avec plus de 5 millions de clés vendues à ce jour, ***Ledger*** se positionne comme leader sur son marché et sécurise plus de 15 % des cryptomonnaies détenues dans le monde (dont 3 à 5 % en France). Les dernières fonctionnalités proposées par le logiciel ***Ledger*** Live facilitent l'achat et le transfert de cryptomonnaies, ce qui permet de répondre aux solutions offertes par ses concurrents, tels que Trezor.

Malware 60

Contraction de *malicious software* signifiant « logiciel malveillant », un ***malware*** est un **programme informatique qui vise à prendre le contrôle de l'ordinateur d'un individu sans son consentement** dans le but de lui soutirer des informations ou d'utiliser des fonctionnalités de son appareil.

Également appelée « cryptojacking », la principale utilisation des ***malwares*** dans l'écosystème des cryptomonnaies a pour objectif d'accaparer la puissance de calcul d'ordinateurs d'individus pour faire du *minage* (→ 11) et ainsi récupérer les récompenses. La méthode de l'hameçonnage demeure à ce jour la plus utilisée pour mettre en place ces ***malwares***. En pratique, le cybercriminel envoie un mail d'apparence officielle à des utilisateurs en leur demandant de cliquer sur un lien. Lorsque la victime ouvre celui-ci, un logiciel de cryptominage se télécharge automatiquement sur son appareil sans qu'il s'en aperçoive. Une fois téléchargé, le logiciel s'exécutera en arrière-plan à chaque fois que l'appareil sera en fonctionnement.

Depuis plusieurs années, le nombre de cryptomalwares créés est en constante augmentation et a dépassé 139 millions en 2022. En effet, les *halvings* (→ 28) successifs augmentant la difficulté du minage (nécessitant donc plus de puissance de calcul) combinée à un prix du bitcoin en forte croissance (donc des récompenses plus importantes pour les mineurs) encouragent la création de tels logiciels.

61 Pair-à-pair

Le ***pair-à-pair*** est un **réseau informatique dans lequel chaque *nœud*** (→ 33) **communique et échange des données directement avec les autres nœuds** sans passer par un serveur central. Ce terme peut également être rencontré dans sa version anglaise *peer-to-peer* ou dans sa version abrégée « P2P ».

Ce modèle est l'opposé du modèle client-serveur dans lequel chaque nœud souhaitant échanger des informations passe par un serveur qui centralise puis redistribue les données aux autres utilisateurs.

Il existe deux principaux types de réseaux ***pair-à-pair*** :

1. **Le modèle partiellement centralisé** : il possède un serveur central qui met en relation les utilisateurs. Le serveur redirige les requêtes pour faire correspondre les offreurs de services avec les demandeurs.
2. **Le modèle décentralisé** : les connexions et les requêtes entre les utilisateurs s'opèrent sans aucun intermédiaire.

Ces réseaux offrent une plus grande fiabilité que le modèle client-serveur, car ils ne dépendent pas d'une seule entité qui pourrait être défaillante. De plus, ce modèle permet une redondance des données qui sont stockées sur plusieurs nœuds en même temps et garantissent donc l'intégrité des informations. Les réseaux Bitcoin et Ethereum s'appuient sur ces méthodes de distribution pour permettre les échanges de cryptomonnaies et conserver l'historique des transactions.

Scam 62

Signifiant « escroquerie », un ***scam*** est **une arnaque visant à extorquer de l'argent à un ou plusieurs utilisateurs**.

Ces arnaques sont très répandues dans l'écosystème des cryptomonnaies du fait de la faible réglementation en vigueur et de sa décentralisation. Elles peuvent revêtir de nombreuses formes différentes, mais se présentent souvent comme des opportunités d'investissement trompeuses. Il peut par exemple s'agir d'une fausse levée de fonds telle qu'une *ICO* (→ 45), où une entité propose des contreparties très rentables contre l'achat de ses actifs. Une fois l'ICO factice finalisée, les porteurs de projet disparaissent avec l'ensemble de l'argent récolté pendant l'opération.

Dans cet écosystème décentralisé où l'investisseur est le seul responsable de ses décisions, il est donc important de savoir reconnaître une fausse opportunité d'investissement à travers plusieurs faisceaux d'indices :

1. L'*analyse fondamentale* (→ 66) des projets : un *white paper* (→ 23) structuré et exhaustif est un bon indicateur par exemple.
2. Le volume de transactions : un volume journalier irrégulier avec des absences de transactions durant plusieurs heures peut alerter sur le caractère suspect de l'actif. Pour vérifier ces informations, vous avez à disposition plusieurs sites tels que *EtherScan*, *Poocoin* et *BSCScan*.
3. Sa présence sur les plateformes d'échanges : un projet solide sera habituellement présent sur de nombreuses plateformes telles que Binance ou Kraken qui auront référencé son actif.

63 Signature numérique

La ***signature numérique*** désigne une **méthode d'authentification et de sécurisation** essentielle dans le fonctionnement des blockchains. Elle permet de connaître avec certitude l'adresse émettrice d'un message ou d'une transaction et de les relier à un certificat.

Il est important de distinguer la ***signature numérique*** de la signature électronique. Cette dernière désigne la version digitale de la signature manuscrite classique. Le terme de signature électronique entend la signature en ligne possédant une valeur juridique.

La ***signature numérique*** utilise quant à elle les techniques de *cryptographie* (→57) asymétrique, c'est-à-dire l'usage d'une clé privée et d'une clé publique pour chiffrer et déchiffrer les messages afin de permettre l'authentification des émetteurs. Cette méthode permet d'éviter le recours à un tiers pour valider l'origine d'une transaction comme le font les banques traditionnelles.

La ***signature numérique*** est par exemple utilisée pour les transactions sur la blockchain Bitcoin. Pour qu'une transaction se réalise sur ce réseau, il faut que l'utilisateur signe avec sa clé privée son transfert, celui-ci sera vérifié par les validateurs à l'aide des clés publiques.

Trustless 64

Signifiant « sans tiers de confiance », le terme ***trustless*** est **une des caractéristiques fondamentales de la blockchain**. Les individus échangent entre eux sans la nécessité de se faire confiance mutuellement et sans avoir recours à des tiers.

Pour comprendre, il est important de comparer le système traditionnel et celui de la blockchain. Prenons un exemple : dans le cadre d'un achat immobilier, l'acquéreur et le vendeur ne se font pas mutuellement confiance sur la transaction et leur bonne foi. Ils font donc appel à un notaire qui garantit les éléments contractuels (prix d'achat, délai de règlement, spécificités du bien) et qui pourra être mobilisé dans le cas d'un recours ultérieur.

Sur la blockchain, les individus ne se font pas non plus mutuellement confiance, mais croient au système dans sa globalité. Son fonctionnement permet ainsi de se passer d'un tiers, car la sécurité des transactions est assurée et distribuée à l'ensemble des utilisateurs. La confiance ne repose sur aucune personne individuelle, mais sur un collectif : chaque utilisateur a la capacité de vérifier et de valider les transactions sur la blockchain réalisées par d'autres.

65 ZKP (Zero knowledge proof)

Signifiant « preuve à divulgation nulle de connaissance », le ***zero knowledge proof*** est un protocole offrant un haut niveau de confidentialité, permettant à un individu de **prouver la possession d'une information ou son authenticité sans révéler l'entièreté de cette dernière**.

Dans l'écosystème, ce protocole est utilisé pour valider non seulement la possession d'informations lors des transactions, mais aussi pour prouver la validité d'une transaction sans révéler certains renseignements comme le montant, l'adresse publique des protagonistes ou des détails tels que la date et l'heure de l'échange.

Les preuves de connaissances nulles, également appelées « Protocoles ZK », peuvent être interactives ou non interactives. Dans un protocole interactif, le « prouveur » et le « vérificateur » doivent échanger plusieurs messages. Dans un protocole non interactif, le « prouveur » peut générer une preuve qui peut être vérifiée par n'importe qui à tout moment.

Des organisations comme Zcash et Monero utilisent le ***zero knowledge proof*** pour proposer à leurs clients de transférer des fonds anonymement sans impacter la sécurité du transfert grâce à la mise en place de *smart contracts* (→ 17). Au-delà de l'utilisation de données sensibles, le ***zero knowledge proof*** peut également être utilisé pour prouver des déclarations plus générales, comme la résolution d'un problème complexe, sans révéler la solution elle-même. Ce système de vérification

pourrait s'appliquer à diverses situations du quotidien, telles que permettre à une personne de prouver sa majorité sans révéler son âge ou démontrer sa solvabilité sans transmettre ses déclarations de revenus lors de la location d'un appartement par exemple.

Chapitre 5

Un écosystème qui puise sa source de la finance traditionnelle

Les cryptoactifs, et plus largement la finance décentralisée, prennent racine dans la finance traditionnelle en proposant un nouveau modèle de croissance et de partage des richesses. Les connaissances et compétences développées depuis des années sont reprises et adaptées pour répondre aux besoins des néo-investisseurs. Nous proposons donc une sélection de termes issus de la finance traditionnelle, qui jouent un rôle tout particulier dans l'écosystème des cryptoactifs.

66 Analyse fondamentale

L'***analyse fondamentale*** est **l'étude de la valeur intrinsèque d'un actif** basée sur des éléments essentiels du projet.

Voici quelques-uns de ces éléments :

1. **Le marché et sa tendance de fond** : la taille du marché visé ainsi que la concurrence à laquelle le projet fera face.
2. **Les métriques du projet** : les informations économiques et financières du projet telles que sa capitalisation ou encore le nombre de jetons émis et distribués.
3. **La proposition de valeur** : des documents tels que la *roadmap* (→ 15) et le *white paper* (→ 23) proposent la description la plus exhaustive du projet.
4. **Les membres du projet** : des équipes de développement compétentes et reconnues ainsi que des parties prenantes (publiques ou privées) peuvent également témoigner de la robustesse d'un projet.

Lorsque l'on parle d'***analyse fondamentale***, nous sommes souvent tentés de mentionner son corollaire : *l'analyse technique* (→ 67). En réalité, l'***analyse fondamentale*** et l'analyse technique sont deux faces d'une même pièce. Chacune vient compléter l'autre et apporte un autre regard.

Analyse technique 67

L'***analyse technique***, souvent utilisée par les traders, est **l'étude d'un actif par l'historique de son cours**. L'objectif est d'analyser graphiquement le prix de marché pour anticiper les futurs mouvements de celui-ci.

Dans un marché aussi volatil que celui des *cryptomonnaies* (→ 6), une ***analyse technique*** performante permet d'estimer les futures variations du prix. Applicable à différentes échelles de temps, l'analyste s'appuie sur des indicateurs techniques qui lui permettent d'acquérir de multiples informations sur l'évolution possible des cours : l'horizon de temps, l'intensité du mouvement et sa tendance.

Le type de graphique principalement utilisé dans ce cadre est la bougie japonaise, complétée par les figures de chartisme qui, grâce à des modèles historiques, permettent aux analystes d'envisager les mouvements des cours des actifs. Ces modèles ont été développés au cours du xviiie siècle et sont souvent attribués à Munehissa Homa, un spéculateur japonais.

68 Arbitrage

L'***arbitrage*** est une **stratégie d'investissement qui consiste principalement à profiter de la différence de prix d'un actif entre deux plateformes d'échange** en réalisant des opérations d'achat-revente. D'autres types d'***arbitrages*** plus complexes existent également.

La *volatilité* (→ 83) du marché des cryptoactifs est particulièrement propice à cette méthode. Contrairement à une stratégie d'investissement à long terme, où la perte peut être le résultat d'une mauvaise *analyse fondamentale* (→ 66), le risque de l'***arbitrage*** est de ne pas réaliser la transaction suffisamment rapidement. Cette latence peut ainsi conduire à revendre un actif à un prix similaire ou même supérieur. Il faut donc veiller à réaliser l'opération sur un réseau non congestionné.

Il est important d'intégrer le coût total de l'opération pour estimer si l'***arbitrage*** sera bénéfique. En effet, l'écart de prix d'un actif sur deux plateformes ne garantit pas un gain *in fine* : il faut y intégrer les frais de transaction.

CBDC (Central Bank Digital Currency)

69

Une ***CBDC***, également appelée MNBC pour « monnaie numérique de banque centrale », est une **monnaie fiduciaire qui se présente sous une forme digitale et est régie par une banque centrale**. Contrairement aux monnaies numériques comme le bitcoin, une ***CBDC*** a donc un cours légal.

Traditionnellement, la monnaie existe sous deux formes : scripturale (elle prend la forme d'écritures sur les comptes bancaires et n'a pas de réalité tangible) et fiduciaire (elle prend la forme des pièces et des billets de banque).

Une ***CBDC*** représente ainsi une troisième forme de monnaie qui se distingue des deux autres en permettant simultanément deux éléments : des échanges directement d'un agent à un autre sans intervention des banques ou États et l'absence de support physique. La monnaie numérique est en quelque sorte la digitalisation de la monnaie fiduciaire. Pour cela, elle utilise le protocole *pair-à-pair* (→ 61) à l'instar du Bitcoin.

La Banque centrale européenne (BCE) expérimente actuellement l'idée d'un euro numérique qui pourrait voir le jour dès 2026. Elle distingue deux types de monnaies numériques :

1. Une ***CBDC*** de gros ou interbancaire, qui sera utilisée par la banque centrale et les banques commerciales.
2. Une ***CBDC*** de détail, qui sera utilisée par tous pour les transactions au quotidien.

Pour résumer : la monnaie numérique se distingue des *cryptomonnaies* (→ 6), car elle est contrôlée et gérée par une institution publique (une banque centrale) qui assure son bon fonctionnement et sa valeur dans le temps. Elle se distingue des *stablecoins* (→ 18) qui dépendent d'une entité émettrice et ne sont pas garantis. Elle se distingue de la monnaie scripturale dans le sens où elle ne requiert pas l'intervention d'intermédiaire (les banques) lors des échanges et se distingue de la monnaie fiduciaire puisqu'elle n'est pas physique.

Dollar Cost Averaging (DCA)

70

Signifiant « étalement des coûts en dollar », le ***DCA*** est une **méthode de placement progressive consistant à investir un montant identique sur un même actif à intervalles réguliers**.

Cette stratégie d'investissement programmée limite le risque lié à la volatilité des actifs en lissant le prix moyen d'achat. En répartissant son investissement total sur une longue période, le prix d'achat moyen de l'actif a une forte probabilité d'être plus intéressant qu'avec une stratégie d'achat en un seul ordre. Il peut être judicieux de mettre en place cette méthode après une importante correction du cours de l'actif, ce qui permet d'obtenir une rentabilité plus importante grâce aux premières positions.

Cette méthode est souvent conseillée pour les investisseurs qui n'ont pas une connaissance parfaite des fluctuations du marché et ne souhaitent pas allouer de temps à une *analyse technique* (→ 67) poussée. Cette méthode peut par ailleurs être mise en place automatiquement sur la plupart des plateformes d'échange.

71 ETF (Exchange Traded Fund)

Signifiant « fonds négociés en bourse », l'***ETF*** est un **produit financier qui réplique la performance d'un ou plusieurs actifs** permettant aux acteurs d'investir sur leur cours sans les acquérir.

Le 10 janvier 2024, la *SEC* (→ 88) a autorisé 11 ***ETF*** spot adossés au bitcoin, proposés par les plus grands fonds d'investissement du monde parmi lesquels BlackRock et Fidelity. En mars 2024, ces derniers représentaient 59 milliards de dollars (soit près de 4 % de l'offre totale de bitcoins).

Également appelé *tracker*, l'***ETF*** est simple d'accès et permet par exemple à un investisseur de procéder à des opérations d'achat et revente sur le cours du bitcoin directement depuis ses courtiers traditionnels sans avoir à utiliser les plateformes d'échange de cryptomonnaies.

Investir sur le cours du bitcoin par le biais d'un ***ETF*** s'avère moins risqué que d'acquérir directement l'actif puisqu'une société s'assure des transactions, et l'investisseur n'est pas responsable du stockage et de la sécurisation de ses actifs. En contrepartie, la rentabilité de l'investissement sera plus faible puisqu'amputée par les frais de gestion du fournisseur de services financiers. De plus, le nombre d'actifs disponibles pour l'investissement est plus faible que le marché global des cryptomonnaies puisque la liste est restreinte à la sélection du fonds d'investissement.

Flat tax 72

Signifiant « taxe forfaitaire », la ***flat tax*** est le **terme anglais définissant le prélèvement forfaitaire unique (PFU) en France**. Réformé depuis le 1er janvier 2018 sous le gouvernement Macron, ce dispositif vise à simplifier la fiscalité en instaurant un impôt unique au taux forfaitaire de 30 %, incluant 12,8 % d'impôt sur le revenu et 17,2 % de prélèvements sociaux.

Cette taxe concerne les revenus issus de placements financiers mobiliers (actions, parts sociales, obligations, titres de créance et comptes à terme), les plus-values de cession de valeurs mobilières, l'assurance-vie, le plan épargne logement (PEL) et le compte épargne logement (CEL). Une plus-value désigne l'augmentation de la valeur d'un actif entre sa date d'acquisition et sa date de vente ou de cession.

À renseigner lors de la déclaration d'impôt sur les revenus N-1 via l'annexe no 2086 (cessions d'actifs numériques), la plus-value générée par la vente d'actifs numériques est à déclarer au même titre que l'ouverture, la détention, l'utilisation et la clôture des comptes d'actifs numériques détenus à l'étranger.

73 FOREX

Abréviation de *Foreign Exchange* signifiant « échange de devises », le ***FOREX*** est **le marché des changes**. Sur ce dernier, les devises du monde entier sont échangées à un taux actualisé en continu.

Ce marché est dit « de gré à gré », c'est-à-dire qu'il est entièrement décentralisé et ne nécessite pas d'intermédiaire. Il existe deux types d'opérations principales sur le ***FOREX*** : les opérations dites *spot* également appelées « au comptant » qui consistent à acheter des devises au cours actuel du marché, et les opérations dites *forwards* ou « à terme » qui consistent à négocier à un instant donné le prix, la quantité et la date ultérieure d'achat d'une devise.

En 2022, le rapport de la Banque des règlements internationaux (BRI) estimait le volume des échanges à près de 7 500 milliards de dollars par jour, le propulsant ainsi au premier rang des marchés les plus importants du monde en matière de transactions. Les deux monnaies les plus échangées dans le monde sont le dollar (présent dans 88 % des échanges de paires) et l'euro (présent dans 31 %).

Évidemment, les acteurs de ce marché sont très rarement des investisseurs particuliers. Il s'agit plutôt d'institutions financières importantes telles que le Fonds monétaire international (FMI), la Banque mondiale, les banques commerciales et les fonds d'investissement.

Gestion active / Gestion passive 74

Dans l'univers des cryptomonnaies, **la *gestion active* et la *gestion passive* sont deux stratégies d'investissement opposées qui permettent de générer des revenus**.

La première, dite « active », est une gestion qui consiste à investir ou échanger un actif en spéculant sur l'évolution à la hausse ou à la baisse du prix. Pour cela, une *analyse fondamentale* (→ 66) du projet ou une *analyse technique* (→ 67) du prix de l'actif doit être effectuée. Cette stratégie permet de profiter de la volatilité du marché et d'obtenir des rendements conséquents avec néanmoins un risque important. En effet, le gestionnaire doit rester constamment attentif au marché et n'a aucune garantie des gains qui seront générés à la suite de la stratégie mise en place. Pire, tout ou partie de ses investissements peuvent être perdus si le cours de l'actif dévie des anticipations.

Le deuxième type de gestion dite « passive » est principalement destiné à développer de nouvelles sources de revenus en utilisant les produits de placement proposés par les fournisseurs de services financiers. Cette alternative est moins risquée que la ***gestion active*** et ne nécessite pas une veille constante, mais génère en moyenne des rendements moins importants. Les stratégies passives les plus connues sont le *staking* (→ 51) qui consiste à verrouiller une partie de ces actifs contre des intérêts et le *lending* (→ 50) qui consiste à prêter des actifs contre des intérêts.

75 Liquidité

La ***liquidité*** désigne **la quantité d'un actif disponible sur une plateforme d'échange** à un instant donné.

Les plateformes disposent d'un certain nombre d'unités de chaque actif qui évolue selon les transactions. Plus cette enveloppe est conséquente, plus le marché est dit liquide, ce qui permettra l'achat et la vente de l'actif rapidement à un prix relativement fixe. À l'inverse, une plateforme d'échange avec une faible ***liquidité*** pour un actif donné ne permettra pas la vente instantanée au prix souhaité. Un ordre de vente ne trouvant pas d'acheteur au prix demandé ne sera pas exécuté, laissant le vendeur dans l'attente avec la possibilité de voir la valeur de l'actif baisser sans avoir réussi à vendre.

Au niveau global, si un actif n'est pas liquide (c'est-à-dire que sa quantité est limitée), l'acte d'achat ou de vente de celui-ci aura un impact sur son prix, le faisant évoluer à la hausse dans le cas d'un ordre d'achat et à la baisse dans le cas d'un ordre de vente.

Listing 76

Signifiant « référencement », le ***listing*** d'une cryptomonnaie est **la mise à disposition d'un actif sur une plateforme d'échange afin que celui-ci puisse être négocié**.

Pour un nouveau projet, le ***listing*** de son jeton sur une plateforme ne garantit pas son référencement sur toutes les autres. En effet, chaque *exchange* (→ 9) fixe ses conditions et ses critères de sélection pour le ***listing*** d'un actif, cela peut être la capitalisation, la viabilité du projet ou la notoriété de celui-ci sur les réseaux sociaux.

Généralement, un *token* est d'abord listé sur une plateforme d'échange secondaire et si les volumes de transactions deviennent suffisamment élevés, les plateformes d'échange les plus importantes comme Binance ou Kraken décident à leur tour d'annoncer son ***listing*** sur leurs plateformes.

Véritable gage de qualité pour un projet, toutes les cryptomonnaies existantes ne sont pas forcément listées sur une plateforme d'échange, ce qui permet de réaliser un premier filtre entre les projets sérieux et les *scams* (→ 62). Lorsqu'un actif est référencé, et plus particulièrement sur une plateforme d'échange reconnue, il n'est pas rare de voir son prix s'envoler en raison de l'achat massif effectué par de nombreux investisseurs présents sur cette plateforme.

À l'inverse, le phénomène de « delisting » existe, à savoir le déréférencement d'un actif des plateformes d'échange, qui peut être justifié par différentes raisons juridiques ou financières.

77 Margin trading

Signifiant « négociation sur marge », le ***margin trading*** est une **méthode consistant à spéculer sur les marchés financiers avec des fonds supérieurs au capital détenu**. Cette méthode est donc étroitement liée au concept d'effet de levier.

Le *trading* consiste à négocier à l'achat ou à la vente des actifs avec pour objectif d'engranger des bénéfices à l'issue des opérations. Le problème du *trading* « classique » réside dans le fait que l'investisseur ne peut engager que ses propres fonds et est donc limité en matière de gains (et de pertes également). Ainsi, s'il réussit à faire une opération lui faisant gagner 10 % sur ses opérations, son gain final sera drastiquement différent s'il a investi 1 000 euros ou 1 million d'euros.

Pour pallier ce problème, les *exchanges* (→ 9) proposent aux investisseurs le concept de ***margin trading***. Pour le marché des cryptomonnaies, cela signifie que les plateformes suggèrent aux investisseurs d'emprunter des fonds permettant d'augmenter leurs positions et par conséquent d'accroître le résultat, qu'il soit positif ou négatif.

Market cap
(Market capitalisation)

78

Signifiant « capitalisation du marché », le ***market cap*** désigne **la valeur totale d'un marché ou d'un actif à un instant donné**.

Parce que le marché des cryptomonnaies est en cotation continue, le ***market cap*** n'est jamais fixe. Cet indicateur se calcule en multipliant la quantité de tous les actifs en circulation par le prix unitaire de ceux-ci. Au moment de la rédaction de cet ouvrage, l'offre de bitcoins en circulation est de 19 678 293 BTC au prix de 69 895 $, soit une capitalisation de 1 375 414 289 235 $. Ce chiffre évolue en permanence selon le nombre de nouveaux bitcoins mis en circulation et leur prix unitaire.

À noter que si le prix unitaire des cryptomonnaies sera toujours variable, le nombre de jetons en circulation peut être fixe selon les règles définies par les protocoles. C'est le cas de Bitcoin qui propose une offre totale maximale de 21 millions d'unités. Une fois l'offre totale mise en circulation, le ***market cap*** de Bitcoin ne dépendra donc plus que de son prix et donc de la loi de l'offre et de la demande.

Cet indicateur permet d'informer les investisseurs sur le potentiel d'un actif. À titre d'exemple, un projet qui dispose d'un ***market cap*** très élevé peut s'avérer moins risqué qu'un autre, car il sera moins sujet à une volatilité importante.

Gage d'enthousiasme envers un actif, le ***market cap*** peut également permettre de connaître la confiance accordée à la totalité d'un marché. À l'heure de la rédaction de ce livre, la capitalisation totale du marché est d'environ 2 640 000 000 000 $. Nous pouvons donc en déduire que Bitcoin représente à cet instant environ 52 % de la valeur totale du marché des cryptomonnaies, on parle également de *dominance* (→ 93). Notons néanmoins que ce ratio est particulièrement changeant selon les cycles économiques des cryptomonnaies.*

OTC (Over The Counter) 79

Signifiant «hors cote», un marché dit «***OTC***», également appelé «marché de gré à gré», **permet la négociation et l'échange d'actifs ou de titres directement entre les parties**, sans l'intervention d'un intermédiaire financier.

Ce marché permet la réalisation de transactions anonymes et occultes sur la nature des contrats, contrairement à un échange sur une plateforme qui rend des comptes aux organismes de contrôle. Il permet également le passage d'ordres à des conditions contractuelles plus flexibles que sur les marchés contrôlés puisque les instruments financiers proposés sont plus nombreux et les frais de transactions moins importants.

Le principal inconvénient d'un marché de gré à gré réside dans le manque de *liquidité* (→ 75). Il est parfois difficile de faire correspondre l'offre et la demande sur ces marchés, et la durée de recherche peut avoir des conséquences sur les gains potentiels des investisseurs. De plus, il existe un risque de non-conformité des contrats, impactant les acteurs de l'échange. Pour finir, le manque de transparence de ces transactions est contraire aux les fondements philosophiques des cryptomonnaies.

80 Produits dérivés

Également appelé « contrat dérivé », un produit dérivé est un **instrument financier dont la valeur dépend d'un autre actif**, appelé sous-jacent. Ce dernier peut par exemple être une action, une obligation, une matière première, une devise ou un taux d'intérêt.

Présents depuis de nombreuses années sur les marchés financiers traditionnels, les ***produits dérivés*** sont des contrats financiers qui permettent aux investisseurs de spéculer sur les mouvements de prix de l'actif sous-jacent ou de se protéger contre les risques associés à ceux-ci. Les deux produits les plus connus étant les options et les trackers.

Plus récemment, ces ***produits dérivés*** ont trouvé leur place sur le marché des cryptoactifs. Sur ce dernier, les ***produits dérivés*** sont proposés aux traders et investisseurs via des plateformes d'échange spécialisées.

Il existe différents types de ***produits dérivés*** dans ce domaine comme les contrats à terme (aussi appelés *futures*) et les options. Ces instruments permettent aux participants du marché de spéculer sur les mouvements futurs des prix des cryptoactifs ou de se couvrir contre les fortes variations de ces prix. Pour finir, il existe également des ***produits dérivés*** permettant de spéculer sur la volatilité des cryptoactifs appelés *move contracts*.

Robot de trading 81

Également appelé *bot de trading*, un ***robot de trading*** est un **logiciel permettant l'exécution automatique d'ordres d'achat et de vente sur les marchés selon des règles définies préalablement**.

Les robots de trading ont considérablement facilité le travail d'analyse et de gestion des opérations financières. Ils ont la capacité de prendre des décisions autonomes selon l'évolution des cours des actifs et de réaliser des transactions avec trois avantages majeurs :

1. Ils fonctionnent en continu.
2. Ils peuvent passer un nombre d'ordres bien supérieur à celui d'un humain.
3. Ils poursuivent constamment la stratégie définie sans risque de variations liées à des acceptations humaines telles que le stress ou la fatigue.

Généralement proposé par des entreprises privées sous forme d'abonnement mensuel, le robot peut être développé par un particulier et connecté à une plateforme d'échange via un *API* (→ 38).

Les robots de trading peuvent être utilisés par des traders de métier, mais également par des investisseurs néophytes. À titre d'exemple, la stratégie *DCA* (→ 70) peut tout à fait être mise en place par ce procédé automatisé.

82 ROI (Return On Investment)

Signifiant « retour sur investissement », le ***ROI*** est **un ratio qui détermine le rendement d'un investissement financier**. Cet indicateur permet de comparer les différents investissements afin de prendre la meilleure décision d'achat.

Le ***ROI*** informe sur le niveau de bénéfice obtenu à partir d'une somme investie et se calcule par la formule suivante :

ROI = (Gain ou Perte de l'investissement - Coût de l'investissement)/Coût de l'investissement

Le retour sur investissement peut s'exprimer selon **trois niveaux** :

1. **Brut** : lorsque seul le coût d'acquisition est pris en compte.
2. **Net** : lorsqu'au coût d'acquisition sont ajoutés les coûts supplémentaires de l'investissement comme les frais de transaction ou de détention d'actifs (il peut s'agir de frais ponctionnés par les plateformes par exemple).
3. **Net-Net** : lorsque la fiscalité est déduite du ***ROI*** Net.

Volatilité 83

La ***volatilité*** est une **mesure de l'amplitude des variations de la valeur d'un actif financier**. On peut mesurer la ***volatilité*** sur différentes échelles de temps allant d'une journée à plusieurs années.

Traditionnellement, on parle de ***volatilité*** forte lorsque l'indicateur est supérieur à 8 % (les marchés des actions et des cryptomonnaies sont considérés comme volatils). À l'inverse, la ***volatilité*** est dite « faible » lorsque le prix des actifs est peu mobile donc inférieur à 8 % sur une période donnée (c'est le cas du marché des obligations d'État).

En théorie économique, la ***volatilité*** d'un actif est associée à la notion de risque : plus un actif est volatil, plus il est difficile de prévoir son prix futur et donc son rendement. L'un des indicateurs de ***volatilité*** les plus connus est le VIX (Volatility Index) qui est l'indicateur de ***volatilité*** du marché américain S&P 500.

Il est important de distinguer deux types de ***volatilité*** :

1. **La *volatilité* historique** : on parle de ***volatilité*** historique ou ***volatilité*** rétrospective lorsque l'on compare l'écart-type d'un actif financier par rapport à son prix moyen constaté sur une période définie.
2. **La *volatilité* implicite** : la ***volatilité*** implicite correspond à la ***volatilité*** future d'un actif financier anticipée par les agents économiques. Cette ***volatilité*** est reflétée dans le prix des options des actifs.

Chapitre 6

Les organismes institutionnels de l'écosystème

Depuis plusieurs années, de nombreuses institutions s'organisent pour réguler et protéger les investisseurs dans l'écosystème crypto. Certains organismes préexistaient aux premières cryptomonnaies et se sont adaptés pour répondre à ces nouveaux besoins. D'autres se sont créés spécifiquement pour cet écosystème afin d'adresser des sujets jusqu'alors orphelins. Ce chapitre vous propose un tour d'horizon des acteurs majeurs en France et à l'international.

84 ADAN (Association de développement pour les actifs numériques)

Créée en 2020, l'***ADAN*** a pour objectif de **représenter le secteur *du Web 3.0*** (→ 22) auprès des pouvoirs publics et de la société civile en France.

L'***ADAN*** s'est fixé quatre missions principales :

1. Soutenir les acteurs du secteur.
2. Participer à la construction de la réglementation française et européenne.
3. Bâtir des ponts entre les institutions et les acteurs du secteur.
4. Démocratiser la technologie blockchain et les cryptomonnaies.

L'association est gérée par un conseil d'administration composé de quinze membres qui sont chargés de l'orientation des missions de l'***ADAN*** et de sa gestion financière. Les membres sont élus pour un mandat de deux ans.

AMF (Autorité des marchés financiers) 85

L'***AMF*** est **un organisme de contrôle et de réglementation français des produits d'épargne et des marchés financiers**. Cette autorité publique indépendante a été créée en 2003 par Francis Mer, ministre de l'Économie, des Finances et de l'Industrie.

Elle veille à la **protection de l'épargne** investie en produits financiers, au **bon déroulement des opérations financières** et à la **transparence des informations**. Elle propose également un dispositif de médiation entre les épargnants et les intermédiaires financiers en cas de litige.

L'équivalent américain de l'***AMF*** est la *SEC* (→ 88) qui est considérée comme le gendarme des marchés américains.

86 Banque centrale

Une ***banque centrale*** est une **institution publique en charge de conduire la politique monétaire pour un pays ou un groupe de pays**. La ***banque centrale*** est également appelée « la banque des banques ».

Parmi les plus importantes, nous pouvons citer la BCE (***Banque centrale*** européenne) qui est l'organe central pour les vingt pays de la zone euro, la FED (pour *Federal reserve*) aux États-Unis, considérée comme la plus influente du monde et la banque d'Angleterre (BoE pour *Bank of England*), l'une des plus anciennes, créée au xviie siècle.

Les objectifs des banques centrales sont d'assurer la stabilité des prix, la valeur de la monnaie sur la scène internationale et l'emploi. Pour ce faire, elles contrôlent la monnaie et font varier sa quantité en circulation.

Le développement des cryptomonnaies oblige à repenser le rôle des banques centrales et à imaginer des innovations dans le domaine monétaire. Depuis quelques années, une réflexion globale est en cours portant sur la création d'une monnaie numérique de ***banque centrale*** ou *CBDC* (→ 69) afin de répondre aux nouveaux besoins des consommateurs.

PSAN (Prestataires de services en actifs numériques) 87

Le ***PSAN*** est un **statut créé en France en 2019 avec la loi PACTE** (Plan d'action pour la croissance et la transformation des entreprises) qui **vise à lever les obstacles à la croissance des organismes proposant des services pour les actifs numériques**. Ce statut est octroyé par *l'AMF* (→ 85). Coinhouse fut la première enregistrée en tant que ***PSAN*** le 17 mars 2020 (sous le numéro d'enregistrement suivant : E2020-001).

Le statut de ***PSAN*** vise à réglementer quatre types d'activités dont la conservation d'actifs numériques pour le compte d'un tiers, la gestion et l'exploitation d'une plateforme d'échange d'actifs numériques, l'achat et la vente d'actifs numériques et enfin les activités de conseil et de gestion de portefeuille.

L'enregistrement de ***PSAN*** est une formalité administrative obligatoire pour toute entreprise exerçant une ou plusieurs des activités suivantes pour le compte de ses clients ou d'autrui :

1. La conservation d'actifs numériques.
2. L'achat ou la vente d'actifs numériques en monnaie ayant cours légal.
3. L'échange d'actifs numériques contre d'autres actifs numériques.
4. L'exploitation d'une plateforme de négociation d'actifs numériques.

Au-delà de cet enregistrement obligatoire, il est possible d'obtenir un agrément facultatif auprès de l'AMF. Cet agrément est beaucoup plus contraignant que l'enregistrement et demande de nombreuses garanties en matière de protection des investisseurs et d'exigences de fonds propres. Très peu d'entreprises ont obtenu l'agrément à ce jour, la première l'ayant obtenu est Forge (filiale de la Société Générale) le 19 juillet 2023. Un des principaux intérêts de cet agrément est commercial, car il autorise les entreprises à un démarchage beaucoup plus important que celles n'ayant qu'un simple enregistrement.

Ces éléments peuvent être retrouvés dans les articles L54-10-1 à L54-10-5 du CMF (Code monétaire et financier).

SEC (Securities and Exchange Commission) 88

Signifiant « Commission de sécurité et d'échanges », la ***SEC*** est **l'organisme fédéral américain qui veille à la réglementation et aux contrôles des marchés financiers**.

Surnommée « le gendarme de la Bourse », la ***SEC*** est créée le 6 juin 1934 à la suite du grand krach boursier de 1929 afin de veiller à la stabilité des marchés et de protéger les investisseurs des sociétés employant des méthodes peu conventionnelles relatives aux achats et ventes d'actions.

La ***SEC***, dont le siège est à Washington D.C., est dirigée par cinq commissaires nommés pour un quinquennat par le président des États-Unis d'Amérique. Elle supervise quatre divisions chargées de la régulation du marché, le financement des sociétés, la mise en vigueur de la réglementation et la gestion des investissements.

Dans l'écosystème des cryptomonnaies, la ***SEC*** a pour mission de veiller à ce que ces actifs ne soient pas utilisés pour le blanchiment d'argent, la fraude fiscale ou encore le financement du terrorisme. Pour ce faire, elle met en place des mesures de régulation et de contrôle comme l'imposition du *KYC* (→ 58) sur les plateformes d'échange.

La ***SEC*** possède des équivalents dans chaque région du monde et peut être comparée à l'action de l'ESMA (*European Securities and Market Authority*) en Europe et l'AMF (Autorité des marchés financiers) en France.

Chapitre 7

Le jargon de la cryptosphère

Une des forces de l'écosystème des cryptoactifs est de réussir à inclure des profils d'investisseurs et d'entrepreneurs les plus variés, allant du débutant au plus chevronné. Cette communauté éclectique nous offre une terminologie riche et un langage spécifique puisant sa source dans différentes cultures. Dans cet ultime chapitre, nous avons choisi de définir les termes les plus utilisés et représentatifs que vous aurez sûrement l'occasion de retrouver dans vos recherches et vos lectures.

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

Signifiant « Le plus haut de tous les temps », **l'*ATH* désigne la valeur la plus haute atteinte par un actif depuis sa création sur un *exchange*** (→ 9).

Signifiant « Le plus bas de tous les temps », ***l'ATL* désigne la valeur la plus faible atteinte par un actif sur un exchange.** Les ***ATH*** et ***ATL*** sont exprimés en valeurs absolues.

Ces points sont des repères jusqu'à ce qu'une nouvelle référence haute ou basse soit établie.

Le prix variant d'une plateforme à une autre, la valeur attribuée à l'***ATH*** ou l'***ATL*** est donc approximative puisqu'en réalité, il existe un point haut et un point bas différent pour chaque plateforme d'échange. Ces différences de cotation sont une opportunité pour les spéculateurs puisqu'elles permettent de mettre en place une stratégie d'*arbitrage* (→ 68) afin de réaliser des profits.

À titre d'exemple, l'***ATH*** du Bitcoin est actuellement de 64 012 € (70 051 $) atteint le 8 mars 2024 sur la plateforme Coinbase. Il n'est pas rare d'observer un ***ATH*** dont le prix approche un niveau psychologique comme un chiffre rond.

L'***ATL*** est généralement établi au référencement de l'actif sur les plateformes, également appelé *listing* (→ 76). Il peut également survenir à la suite d'un événement perturbant le projet. C'est par exemple ce qui est arrivé au projet Terra

Luna qui avait atteint un ***ATH*** à 119,18 $ sur la plateforme Binance le 5 avril 2022 qui, à la suite d'une défaillance importante, a fortement chuté jusqu'à créer un ***ATL*** à 0,000 05 $ le 17 août 2023 sur l'*exchange* Binance créant ainsi un ***ATL*** historique après une forte croissance.

90 Bag

Signifiant « sac », un ***bag*** désigne en argot une **quantité importante d'un même actif** détenue par un investisseur. Il n'existe pas de consensus sur la quantité minimale à posséder pour qualifier un portefeuille de ***bag***.

Ce terme peut également désigner le **portefeuille global d'un investisseur** composé de différents types d'actifs : cryptomonnaies, *tokens*, *produits dérivés* (→ 80). Dans ce cas, ce terme est synonyme de *stack*.

Bear Market / Bull Market 91

Signifiant « marché baissier », le ***bear market* désigne une période de baisse des prix durable**, tandis que le ***bull market*** qui signifie « marché haussier » désigne une **période de hausse des prix durable**.

Il n'existe pas de consensus précis sur la délimitation d'un ***bear*** ou d'un ***bull market***, mais la plupart des analystes financiers s'accordent sur les deux caractéristiques qui définissent la tendance du prix :

1. **Notable** : en marché baissier, la chute doit être au minimum de 20 % sur les marchés baissiers traditionnels, mais peut atteindre plus de 60 % sur le marché des cryptomonnaies par rapport aux derniers points hauts. En marché haussier, la hausse des prix doit être de plusieurs dizaines de pour cent.
2. **Durable** : en marché baissier comme en marché haussier, le mouvement du prix ne doit pas être ponctuel, mais s'apparenter à une tendance de fond, allant de deux mois à plusieurs années en ***bear market***, tandis qu'en ***bull market***, la hausse dure généralement de quelques semaines à plusieurs mois.

Quelle que soit la tendance, cela ne peut se résumer qu'à une acceptation mathématique et mesurable du phénomène. En effet, il se distingue également par la psychologie du marché et des investisseurs. Au sein des marchés financiers, la confiance et les anticipations sont des facteurs importants parfois irrationnels qui guident les tendances de long terme.

La tendance baissière est souvent imagée par un ours (*bear* en anglais) dont le mode d'attaque est semblable à l'évolution du prix : du haut vers le bas. La tendance haussière est quant à elle souvent symbolisée par un taureau (*bull* en anglais) dont le mode d'attaque est semblable à l'évolution du prix : du bas vers le haut.

Depuis sa création, nous observons que les marchés baissiers interviennent de manière cyclique. Les trois ***bear markets*** que le Bitcoin a connus sont intervenus en 2014, 2018 et 2022. Le dernier ***bull market*** que l'écosystème des cryptomonnaies a connu s'est déroulé entre mars 2020 et fin 2021. Durant quatre-vingt-six semaines, le prix du Bitcoin a évolué de manière très importante, passant de 4000 $ à 69000 $, soit une hausse d'environ 1700 %.

Cypherpunk 92

Le terme ***cypherpunk*** fait référence à un **groupe d'intellectuels, de chercheurs et d'activistes** qui s'est constitué dans les années quatre-vingt et qui **prônait la préservation de la liberté individuelle et de la vie privée grâce à l'usage de la cryptographie**.

Cette dénomination est un mot-valise provenant des termes *cipher* signifiant « chiffrement » et *punk* signifiant « voyou ». Elle est attribuée à l'activiste américaine Jude Milhon en 1992.

Ces militants ont développé une pensée politique critique envers le rôle de l'État souhaitant redonner du pouvoir aux individus et protéger leurs intérêts. Leur idéologie est proche du libertarianisme, courant de pensée qui prône une société fondée sur l'expression des individus et le pluralisme.

Ces acteurs ont grandement contribué au développement de la technologie blockchain et des cryptomonnaies. Un des ***cypherpunks*** les plus influents étant Adam Back, l'inventeur du *hashcash*, un algorithme qui fut repris et modifié avant d'être implémenté dans Bitcoin.

93 Dominance

La ***dominance*** d'un actif est **la prépondérance de sa capitalisation comparativement à celle d'un ou plusieurs autres**. Dans la cryptosphère, on parle le plus souvent de la ***dominance*** bitcoin, pour mesurer son hégémonie face à tous les autres actifs.

La ***dominance*** se calcule par rapport à la capitalisation totale d'un marché. Bien que le bitcoin serve généralement de repère pour cette ***dominance***, celle-ci peut être calculée pour tous les cryptoactifs via la formule :

Dominance de l'actif = capitalisation de l'actif/capitalisation totale du marché des cryptomonnaies

Lors de la rédaction de cet ouvrage, la capitalisation de bitcoin est de 1 375 414 289 235 $ pour une capitalisation totale du marché de 2 640 000 000 000 $, soit une ***dominance*** de bitcoin sur le marché d'environ 52 %.

Fiat 94

Le terme ***fiat*** est utilisé par la cryptosphère pour désigner toutes les **monnaies ayant cours légal et reconnu par un pays ou un ensemble de pays** tels que l'euro ou le dollar. Ce terme est utilisé pour parler de ces monnaies en opposition avec les cryptomonnaies.

Du latin « qu'il soit fait », le mot ***fiat*** renvoie à la notion de l'imposition d'une autorité dans le choix de la monnaie qui sera utilisée comme moyen d'échange. Ce choix est arbitraire, car ces monnaies n'ont pas de valeur intrinsèque. Les monnaies ***fiat*** sont gérées par les *banques centrales* (→ 86).

Cette notion est souvent confondue avec le terme de « monnaie fiduciaire ». D'un point de vue économique, la monnaie fiduciaire représente la forme spécifique des pièces et billets qu'une monnaie ***fiat*** peut prendre.

Le terme ***fiat*** est également utilisé pour critiquer le fonctionnement des monnaies dépendantes d'une autorité qui, selon les objectifs économiques, peut faire évoluer sa valeur sans l'approbation des populations.

95 Flippening

Signifiant « retournement », le ***flippening*** désigne **le revirement majeur potentiel dans l'écosystème des cryptomonnaies intervenant si la capitalisation d'Ethereum dépasse celle de Bitcoin**.

On parle de retournement « potentiel », car il existe actuellement un écart très important entre Bitcoin et Ethereum, et qu'il est impossible de prédire si cette hégémonie sera bousculée un jour. En effet, Bitcoin est depuis toujours la plus grosse capitalisation sur le marché des cryptomonnaies avec une capitalisation de près de 1400 milliards de dollars. Ethereum s'est en revanche fortement développé, devenant structurellement depuis 2016 la deuxième plus importante cryptomonnaie en matière de capitalisation avec près de 430 milliards de dollars à ce jour.

Cet écart impressionnant donne un fort avantage à Bitcoin même si des signaux semblent indiquer qu'un retournement pourrait se produire dans les prochaines années. Depuis 2017, Ethereum voit son nombre de transactions dépasser celles de Bitcoin, notamment grâce à l'émergence de la finance décentralisée et depuis janvier 2019, le nombre de portefeuilles détenant de l'ether (ETH) a dépassé le nombre de portefeuilles détenant du bitcoin (BTC).

Holding 96

Signifiant « conserver », *holder* une cryptomonnaie implique de conserver un actif dans son portefeuille en vue d'un investissement à long terme.

Cette stratégie d'investissement est la plus populaire puisqu'elle ne nécessite pas de grandes connaissances dans le domaine, mais simplement d'acquérir des actifs ayant un fort potentiel à long terme afin de les revendre à un moment opportun. À titre d'exemple, un investisseur ayant acheté 1 bitcoin en 2013 au prix de 287 € pouvait le revendre au prix de 50 000 € en 2021, soit une croissance de 17 400 %.

Pour conserver vos actifs en sécurité, il est conseillé de les transférer sur un *wallet* (→ 21) sécurisé et de ne pas les détenir directement sur les plateformes d'échange. En effet, les plateformes peuvent subir des attaques informatiques ou faire faillite, occasionnant la perte de l'intégralité des fonds à leurs clients à la manière de ce qui est arrivé sur l'*exchange* (→ 9) FTX en novembre 2022.

Pour l'anecdote, il est également possible de voir le terme de *Hodl* dans la cryptosphère pour désigner l'action de conserver ses actifs. Ce terme devenu un mème Internet provient d'un message rédigé par un détenteur de cryptomonnaie connu sous le pseudo de GameKyuubi à la suite du krach de décembre 2013. Probablement en état d'ébriété, il écrit un post intitulé *I am hodling* à la place de *I am holding* afin d'expliquer qu'il comptait maintenir sa position à long terme malgré la forte volatilité. Cette faute deviendra un phénomène Internet célébré le 18 décembre, jour du *Hodl*.

97 Pump/Dump

Signifiant « pompe », un ***pump*** représente une **hausse soudaine et violente du prix**.

Signifiant « décharge », un ***dump*** représente une **baisse brutale et soudaine du prix d'un actif financier**.

Le ***dump*** peut faire suite à une vente massive d'un actif par un gros portefeuille, également appelé *whale* (→ 100). Il peut aussi être la conséquence des ordres de vente programmés par les investisseurs. En effet, de nombreux acteurs utilisent des ordres automatiques dits *stop Loss* permettant de céder un actif à un seuil prédéfini pour réduire leurs pertes lors d'une phase baissière. Ces ordres étant souvent positionnés à des valeurs communes, leur exécution simultanée entraîne un phénomène de ***dump***.

À l'inverse, le ***pump*** peut également être la conséquence d'ordres d'achat exécutés automatiquement à des seuils prédéfinis, souvent communs aux investisseurs. Il peut également être occasionné à la suite d'une annonce importante réalisée par une personnalité influente, une institution ou par l'entreprise qui possède l'actif.

Une manipulation de marché très dangereuse appelée ***pump*** *and* ***dump*** joue avec ces deux phénomènes. Cette technique vise à engranger des bénéfices importants et très rapides par une partie des investisseurs. En pratique, un groupe d'individus s'organise pour acheter massivement un actif afin de faire croître artificiellement son prix. Cette hausse attire de nouveaux investisseurs contribuant à

l'augmentation continue du cours de l'actif. Lorsque le prix atteint le niveau attendu, les protagonistes ayant amorcé cette inflexion vendent massivement l'actif afin de récolter les bénéfices, causant ainsi l'écroulement de son cours et donc la perte du capital des investisseurs nouvellement arrivés sur le marché. Cette méthode, interdite sur les marchés financiers, n'est malheureusement pas contrôlable dans l'écosystème des cryptomonnaies.

98 To the moon

Signifiant « vers la lune », cette expression est souvent employée lorsque **le cours d'une cryptomonnaie évolue subitement à la hausse**. Cette métaphore est utilisée pour motiver la communauté à participer à l'achat d'un actif.

Imagée par une fusée au décollage, cette expression a très souvent été utilisée par Elon Musk lorsqu'il faisait l'éloge du *Dogecoin* pour encourager les investisseurs à le faire atteindre de nouveaux sommets. En réponse aux annonces du milliardaire, le cours du *Dogecoin* a connu de nombreux *pumps* (→97) faisant augmenter son cours de près de 9000 % entre janvier et mai 2021.

Weak hands 99

Signifiant « mains fébriles », une ***weak hand*** caractérise **des investisseurs prenant des décisions de vente hâtives** dès que les cours des actifs diminuent.

La communauté « crypto » est souvent critique envers ces investisseurs, souvent considérés comme inexpérimentés et trop sensibles au cours du marché. Ils sont vus comme incapables de tenir des positions sur le long terme, leurs décisions étant dictées par la peur, l'incertitude et le doute,ces attitudes pouvant être regroupées sous l'acronyme « FUD » pour *fear, uncertainty and doubt*.

Par opposition, nous retrouvons le terme de *diamond hands* pour désigner les investisseurs qui conservent leurs actifs indépendamment des fluctuations du marché.

100 Whale

Signifiant « baleine », une ***whale*** désigne un **détenteur d'une quantité très importante de cryptomonnaies**.

Ces gros portefeuilles peuvent être des particuliers ou des entreprises, tels que des fonds d'investissement ou des fonds spéculatifs. Une baleine peut jouer un rôle important sur les marchés, car elle a le pouvoir de faire varier significativement le cours d'une cryptomonnaie en passant des ordres d'achat ou de vente importants.

À ce jour, les ***whales*** les plus épiées par les investisseurs sont les *Bitcoin* ***whales***. En effet, cette cryptomonnaie est une valeur stratégique à surveiller puisqu'elle représente une part importante dans la capitalisation totale du marché des cryptomonnaies. Même s'il n'y a pas de consensus établi sur le niveau nécessaire pour être défini comme une Bitcoin ***whale***, il est admis qu'un portefeuille détenant 1 000 bitcoins ou plus est considéré comme tel. À date, près de 40 % de l'offre de bitcoins en circulation serait détenu par environ 2 100 portefeuilles considérés comme des ***whales.***

À ce jour, il n'y a pas de consensus sur le nombre d'unités de cryptoactifs à détenir pour être qualifié de ***whale***. Néanmoins, des tentatives de classification des détenteurs ont récemment été proposées, basées sur le nombre de bitcoins détenus.

Nous retrouvons ainsi la classification suivante :

1. **Crevette** (*shrimp*) : moins de 1 BTC.
2. **Crabe** (*crab*) : entre 1 et 10 BTC.
3. **Pieuvre** (*octopus*) : entre 10 et 50 BTC.
4. **Poisson** (*fish*) : entre 50 et 100 BTC.
5. **Dauphin** (*dolphin*) : entre 100 et 500 BTC.
6. **Requin** (*shark*) : entre 500 et 1000 BTC.
7. **Baleine** (***whale***) : entre 1000 et 5000 BTC.
8. **Baleine à bosse** (*humpback*) : plus de 5000 BTC.

Remerciements

Nous tenions à remercier très chaleureusement toutes les personnes, expertes ou jeunes initiées qui par leurs relectures et leurs éclairages croisés ont contribué à rendre cet ouvrage accessible au plus grand nombre.

Martino Bettucci, fondateur du salon IA-WEB3 et enseignant à Alyra et à la Blockchain BS.

Mehdi Jabri, Ingénieur généraliste.

Thibault Da Costa, Consultant Senior pour le Groupe BPCE.

Clémence Lorette, Head of CSM France-Espagne pour Bien'ici.

Charles Moukaga, directeur d'exploitation de la société Profero Transport et Logistique.

Si vous avez apprécié ce livre ou souhaitez échanger avec nous, nous serons ravis de connaître votre avis et de poursuivre les réflexions autour de cet écosystème qui n'a pas fini de se développer et de nous surprendre.

Index

Quentin DEMÉ est économiste et enseignant en macroéconomie, microéconomie et finance notamment à l'université Paris 1 Panthéon-Sorbonne, l'EDHEC et KEDGE.

Depuis plusieurs années, il se consacre à la vulgarisation de l'économie à travers des analyses dans les médias et les Conférences Soufflot, cycle de conférences annuelles gratuites accueillant des personnalités éminentes de l'économie et de l'entrepreneuriat, dont il est le président fondateur.

En 2023, il fonde le congrès UPI, le premier événement annuel sur l'économie et le monde des affaires, qui propose un format novateur mêlant expertise et divertissement.

Kévin RICOULT s'intéresse depuis plusieurs années aux cryptomonnaies et plus largement à la technologie de la blockchain. D'abord en tant qu'investisseur, il développe son expertise sur ces sujets avant de se spécialiser sur la partie technique.

En 2024, il obtient la certification RS6410, témoignant de sa capacité à mettre en œuvre des solutions numériques grâce à la technologie blockchain. Il collabore à la création d'une application décentralisée qui a pour vocation d'être proposée au grand public en 2025.

Ayant à cœur de transmettre ses connaissances, il anime une communauté réunissant à ce jour environ 1 000 investisseurs et entrepreneurs dans le Maine-et-Loire.

GERESO
FORMATION | CONSEIL | ÉDITION

Révélez vos compétences !

100 MOTS POUR COMPRENDRE LES CRYPTOMONNAIES

Les cryptomonnaies ont pris une importance capitale dans l'économie mondiale, jusqu'à faire régulièrement la une de journaux financiers.

Les gouvernements, les institutions, les entreprises et les particuliers leur accordent désormais une place de choix dans leurs réflexions.

Malgré tout, la connaissance du grand public reste encore très restreinte, souvent limitée à quelques notions de base, constituant souvent la principale cause de défiance envers ce secteur.

Avec un double regard économique et pratique, les auteurs ont sélectionné les mots les plus pertinents pour traduire les tendances représentatives de la réalité du terrain.

Dans cet ouvrage simple d'accès, ils permettent au plus grand nombre de s'initier à ces sujets qui ne vont cesser de prendre de l'ampleur dans les prochaines années.

Investir en toute confiance, comprendre les implications technologiques, rester informé sur les évolutions économiques et financières...

Retrouvez le vocabulaire indispensable à la compréhension de l'écosystème des cryptomonnaies.

Quentin DEMÉ
est économiste et enseignant en macroéconomie, microéconomie et finance, notamment à l'université Paris 1 Panthéon-Sorbonne, l'EDHEC et KEDGE.

Kévin RICOULT
est spécialiste de l'écosystème des cryptomonnaies.