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.

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***.

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.