XMR - Monero

Monero (XMR) est une cryptomonnaie open-source qui met l'accent sur la confidentialité, la sécurité et l'intransa□□abilité des transactions. Fondée sur une blockchain dédiée, elle utilise un mécanisme de consensus de preuve de travail (Proof-of-Work). Son objectif principal est d'offrir un moyen d'échange numérique privé, comparable à l'argent liquide, où les détails des transactions sont masqués par défaut pour tous les utilisateurs. Contrairement aux blockchains transparentes comme celle de Bitcoin, Monero utilise plusieurs technologies cryptographiques pour garantir la confidentialité.

Les caractéristiques technologiques clés de Monero incluent :

- **Signatures d'anneau (Ring Signatures)** : Elles permettent de mélanger la signature de l'expéditeur avec d'autres signatures de participants potentiels, rendant impossible l'identification de l'expéditeur réel.
- **Adresses furtives (Stealth Addresses)** : Pour chaque transaction, une adresse de destination unique et éphémère est générée. Cela empêche le suivi des fonds reçus, même si le destinataire est le même.
- **Transactions confidentielles d'anneau (RingCT)** : Cette technologie chiffre le montant des transactions, masquant ainsi la valeur transférée.

Ces mécanismes garantissent que l'expéditeur, le destinataire et le montant de chaque transaction sont cachés des observateurs externes.

Monero utilise l'algorithme de minage RandomX, une variante de preuve de travail conçue pour être résistante aux ASIC (circuits intégrés spécifiques à une application). Cet algorithme favorise le minage par processeur (CPU) et carte graphique (GPU), promouvant ainsi un écosystème minier plus décentralisé et accessible aux particuliers. Le réseau a un temps de bloc moyen d'environ deux minutes.

Concernant la tokenomique, Monero a un approvisionnement quasi illimité en raison de sa "tail emission". Initialement, l'émission de nouveaux XMR était élevée, mais elle a diminué avec le temps. Depuis juin 2022, Monero est entré dans sa phase de "tail emission", où une quantité fixe de 0,6 XMR est émise pour chaque bloc, assurant une faible inflation perpétuelle. Ce mécanisme vise à inciter les mineurs à sécuriser le réseau indéfiniment, sans

dépendre uniquement des frais de transaction. L'approvisionnement total est estimé autour de 18,4 millions de XMR, avec une légère inflation continue.

L'utilité principale du token XMR est de servir de moyen d'échange privé et de faciliter les opérations sur le réseau, notamment le paiement des frais de transaction qui varient en fonction de la congestion du réseau et de la taille des données. La fongibilité est une caractéristique clé de Monero : chaque XMR est interchangeable et indistinguable des autres, car aucune transaction n'est marquée ou 'tachée' par son historique, ce qui le différencie des cryptomonnaies transparentes.

La gouvernance de Monero est décentralisée et communautaire. Il n'y a pas de fondation centralisée dictant la feuille de route. Les priorités de développement émergent du Monero Research Lab, des discussions communautaires et des propositions des contributeurs. Les mises à jour majeures, souvent activées par des hard forks, sont adoptées par la communauté si elle met à jour son logiciel, un processus qui a abouti à un consensus jusqu'à présent.

Monero trouve des cas d'utilisation dans les transactions privées, les envois de fonds internationaux, le commerce en ligne et dans les marchés où la confidentialité financière est primordiale. Il est souvent considéré comme le 'gold standard' des cryptomonnaies axées sur la confidentialité. Cependant, ses caractéristiques de confidentialité ont également suscité des préoccupations réglementaires et conduit à des restrictions sur certaines plateformes d'échange.

En résumé, Monero se distingue par son engagement inébranlable envers la vie privée, la sécurité et la fongibilité, offrant une alternative robuste aux systèmes financiers transparents et centralisés.