XMR - Monero

Monero (XMR) se distingue dans l'écosystème des cryptomonnaies par son engagement fondamental envers la confidentialité et l'anonymat des transactions. Lancée en avril 2014, Monero repose sur le protocole CryptoNote, une évolution du code source de Bytecoin, avec pour ambition d'offrir une monnaie numérique où la vie privée est garantie par défaut pour tous les utilisateurs. Contrairement aux blockchains transparentes comme celle de Bitcoin, où chaque transaction est publiquement enregistrée et potentiellement traçable, Monero utilise un ensemble de technologies cryptographiques avancées pour masquer ces informations.

Les piliers technologiques de Monero sont les signatures en anneau (Ring Signatures), les adresses furtives (Stealth Addresses) et les transactions confidentielles (RingCT). Les signatures en anneau mélangent la transaction de l'expéditeur avec un groupe d'autres signataires possibles, rendant l'identification de la source réelle extrêmement difficile. Les adresses furtives génèrent une adresse unique et temporaire pour chaque transaction, protégeant ainsi l'identité du destinataire réel. Enfin, RingCT chiffre les montants des transactions, assurant la confidentialité financière. Ces mécanismes combinés garantissent que l'expéditeur, le destinataire et le montant de chaque transaction sont dissimulés.

L'utilité principale du token XMR est d'agir comme moyen de paiement au sein du réseau Monero. La confidentialité intégrée de Monero le rend particulièrement attrayant pour les utilisateurs qui souhaitent protéger leurs informations financières contre la surveillance. Cette caractéristique assure également la fongibilité de Monero, signifiant que chaque unité de XMR est interchangeable avec une autre, car aucune pièce ne peut être distinguée ou "souillée" par son historique de transaction.

Sur le plan de la gouvernance et de la sécurité, Monero est un projet open-source et décentralisé, financé par des contributions communautaires via son système de financement participatif (CCS). Il utilise un algorithme de consensus Proof-of-Work (PoW). La particularité de son algorithme de minage, RandomX, est qu'il est conçu pour être résistant aux circuits intégrés spécifiques aux applications (ASIC), favorisant ainsi le minage par CPU et GPU et encourageant une plus grande décentralisation du réseau.

En ce qui concerne le tokenomics de XMR, Monero a une offre totale plafonnée à environ

18,4 millions de jetons. Il n'y a pas de maximum absolu fixé de manière stricte, mais un mécanisme de "tail emission" (émission de queue) a été activé en 2022. Ce système assure une récompense continue aux mineurs avec une faible inflation perpétuelle d'environ 432 XMR par jour, garantissant la sécurité du réseau à long terme, même après que la majeure partie des jetons ait été minée. L'émission initiale était plus élevée et a diminué progressivement.

Les avantages de Monero résident dans sa confidentialité et son anonymat par défaut, sa fongibilité, sa résistance à la censure et sa décentralisation. Cependant, ces mêmes caractéristiques de confidentialité posent des défis réglementaires, entraînant parfois des délistages sur certaines plateformes d'échange. Les limites potentielles incluent la complexité technique pour les nouveaux utilisateurs, la volatilité accrue due à une liquidité parfois plus faible que celle des cryptomonnaies majeures, et les risques liés à la conformité réglementaire.

Les perspectives de Monero restent axées sur le renforcement de sa position en tant que référence des cryptomonnaies axées sur la confidentialité. Son adoption par des utilisateurs privilégiant la vie privée, ainsi que le développement continu de ses technologies de protection, sont des facteurs clés pour sa pérennité. L'écosystème Monero continue d'évoluer, avec des innovations visant à améliorer l'efficacité des transactions et la robustesse de la confidentialité.