Monero ($XMR) : Réseau de paiement décentralisé permettant de conserver un anonymat on-chain.

Monero est une blockchain de Layer 1 dont l'objectif principal est de fournir une infrastructure décentralisée permettant d'effectuer des transactions tout en préservant la vie privée des utilisateurs. Contrairement aux grandes blockchains de L1 comme Bitcoin ou Ethereum, où toutes les transactions sont publiques et traçables, Monero se positionne comme une alternative axée sur la confidentialité par défaut.

- Monero présente plusieurs similitudes avec Bitcoin, notamment son fair launch : aucun préminage et aucune levée de fonds. Le développement du protocole est entièrement communautaire, et toute personne peut contribuer à ce projet open source. Le réseau repose sur un algorithme de Proof-of-Work, permettant aux mineurs de sécuriser la blockchain en échange de récompenses de blocs.
- Contrairement à Bitcoin, les récompenses de blocs de Monero ne sont pas soumises à des halvings. Le protocole maintient une inflation permanente inférieure à 1 %, assurant une rémunération continue des mineurs. Toutefois, l'utilisation du réseau peut réduire cette inflation : lorsque les frais de transaction inclus dans un bloc dépassent la récompense de base, cette dernière est brûlée, et seuls les frais de transaction constituent la récompense du mineur.
- Le jeton XMR est utilisé de manière similaire au Bitcoin, à la fois pour payer les frais de transaction et pour inciter la sécurisation du réseau.
- Monero offre un niveau de confidentialité très élevé et constitue l'un des rares réseaux permettant réellement de préserver l'anonymat on-chain. Cela dit, l'hygiène des utilisateurs reste un facteur clé : le fait que la majorité des XMR soient acquis via des plateformes centralisées (CEX) peut compromettre la confidentialité s'il n'y a pas de bonnes pratiques en amont. De plus, la complexité du protocole et de son utilisation limite son accessibilité au grand public. À cela s'ajoute un risque réglementaire important, plusieurs pays et plateformes ayant restreint ou interdit l'utilisation de Monero.
- Bien qu'il soit un leader du narratif de la confidentialité, Monero demeure un réseau relativement niché. L'attaque de type 51 %, attribuée au protocole Qubic, a mis en lumière le fait que la puissance de calcul sécurisant le réseau est nettement inférieure à celle de Bitcoin. Cet élément est crucial, car le hashrate est directement lié à l'immutabilité et à la résilience d'une blockchain.

Pour conclure, Monero est un protocole qui fonctionne, qui est robuste et qui a démontré sa durabilité dans le temps. Il répond à un besoin réel en matière de

confidentialité financière. Toutefois, son adoption reste freinée par des enjeux réglementaires, une complexité technique élevée et une accessibilité limitée. D’un point de vue utilisateur, Monero est une solution efficace pour la protection de la vie privée. En revanche, du point de vue investissement, le jeton XMR comporte des risques importants liés au cadre réglementaire et à la pression exercée sur les protocoles de confidentialité.