ZEC - Zcash

Zcash (ZEC) est une cryptomonnaie open-source, créée en octobre 2016, qui se positionne comme une alternative axée sur la confidentialité à Bitcoin. Son objectif principal est de résoudre le problème du manque de confidentialité financière de Bitcoin, où toutes les transactions sont publiquement visibles sur la blockchain. Zcash y parvient grâce à l'implémentation des zk-SNARKs (preuves succinctes non interactives à divulgation nulle de connaissance), une technologie cryptographique avancée qui permet de vérifier la validité d'une transaction sans révéler d'informations sensibles telles que l'expéditeur, le destinataire ou le montant.

Le protocole Zcash offre une confidentialité optionnelle, permettant aux utilisateurs de choisir entre deux types d'adresses : les adresses transparentes (t-addrs), qui fonctionnent de manière similaire aux adresses Bitcoin et dont les transactions sont publiques, et les adresses protégées (z-addrs), qui garantissent la confidentialité des transactions. Cette flexibilité permet aux utilisateurs de répondre à des besoins variés, allant de la transparence pour l'audit à la confidentialité totale pour les transactions privées. Cette approche différencie Zcash d'autres cryptomonnaies axées sur la confidentialité où celle-ci est automatique.

Technologiquement, Zcash est un fork de Bitcoin, partageant une base de code similaire et une offre maximale plafonnée à 21 millions de ZEC. Il utilise un mécanisme de consensus de preuve de travail (PoW) avec l'algorithme de minage Equihash, conçu pour être résistant aux ASIC afin de favoriser un minage plus décentralisé. Le temps de bloc est d'environ 75 secondes après la mise à jour Blossom.

Le token ZEC joue un rôle central dans l'écosystème Zcash. Il est utilisé pour sécuriser le réseau par le biais du minage, les mineurs étant récompensés en ZEC pour la validation des blocs et la sécurisation des transactions. De plus, une partie de l'émission de nouveaux ZEC est allouée au financement du développement du protocole, assurant la pérennité et l'évolution du projet sans dépendre uniquement d'investisseurs externes. Cette structure de financement est une approche innovante en matière de gouvernance et de développement durable pour les projets blockchain.

Les cas d'usage de Zcash incluent les transferts personnels, les paiements transfrontaliers,

les dons, et toute situation nécessitant une discrétion financière, y compris pour les transactions commerciales où les entreprises peuvent souhaiter éviter la surveillance de leurs flux financiers.

Cependant, Zcash fait face à des défis. Le secteur des cryptomonnaies axées sur la confidentialité est concurrentiel. De plus, la gestion du projet par une société (Electronic Coin Company) et une fondation, ainsi qu'une taxe sur le minage (bien que son modèle de financement soit considéré comme innovant par certains), peuvent susciter des débats sur la gouvernance et la décentralisation. L'adoption des transactions privées peut également varier en fonction des plateformes d'échange et des considérations réglementaires.

Malgré ces défis, Zcash continue d'innover, comme en témoigne l'augmentation de l'offre protégée de son jeton, faisant de Zcash une option considérée pour les entités institutionnelles recherchant une « confidentialité réglementée ».