ZEC - Zcash

Zcash (ZEC) est une cryptomonnaie et un protocole de blockchain open-source lancé en octobre 2016. Son principal objectif est d'offrir un niveau élevé de confidentialité financière aux utilisateurs, comblant ainsi une lacune perçue dans la transparence par défaut de certaines blockchains comme Bitcoin.

Technologie et Fonctionnement : Au cœur de Zcash se trouve la technologie des preuves à divulgation nulle de connaissance, plus spécifiquement les zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Cette technologie cryptographique permet de prouver qu'une transaction est valide sans divulguer d'informations sensibles. Zcash utilise deux types d'adresses : les « t-addresses » (transparentes), qui fonctionnent de manière similaire aux adresses Bitcoin où les détails de la transaction sont visibles publiquement sur la blockchain, et les « z-addresses » (chiffrées ou privées), qui utilisent les zk-SNARKs pour masquer l'expéditeur, le destinataire et le montant de la transaction. Cette dualité offre une flexibilité sans précédent, permettant aux utilisateurs de choisir le niveau de confidentialité adapté à leurs besoins, qu'il s'agisse de transactions publiques pour la conformité réglementaire ou de transactions privées pour une confidentialité maximale.

Cas d'Usage et Utilité : L'utilité principale de ZEC réside dans sa capacité à permettre des paiements numériques confidentiels. Il peut être utilisé pour des transactions peer-to-peer privées, des transferts transfrontaliers où la discrétion financière est importante, ou encore pour payer les frais de transaction sur le réseau Zcash. La possibilité de divulgation sélective via des « view keys » (clés de visualisation) permet également aux utilisateurs de partager volontairement des détails de transaction avec des auditeurs ou des régulateurs, facilitant ainsi l'intégration dans les cadres réglementaires.

Tokenomics et Gouvernance : Le ZEC, le jeton natif de Zcash, partage plusieurs caractéristiques économiques avec Bitcoin. Il a une offre maximale fixe de 21 millions de jetons. Le ZEC est émis par le biais d'un mécanisme de Preuve de Travail (Proof-of-Work) utilisant l'algorithme Equihash. Le processus de minage récompense les mineurs, avec une partie des récompenses allouée à un fonds de développement pour soutenir la maintenance et l'amélioration du protocole. Le ZEC subit des « halvings » (réductions de moitié des récompenses) périodiques, similaires à Bitcoin, pour ralentir le taux d'émission et maintenir

la rareté. La gouvernance du projet est assurée par un processus de « Zcash Improvement Proposals » (ZIPs) et des mises à jour du réseau, impliquant des organisations comme l'Electric Coin Company (ECC) et la Zcash Foundation, ainsi que la communauté des détenteurs de ZEC.

Avantages et Limites : L'avantage majeur de Zcash est sa confidentialité optionnelle grâce aux zk-SNARKs, offrant une flexibilité supérieure par rapport aux cryptomonnaies strictement transparentes ou strictement privées. Il permet également la divulgation sélective pour des raisons de conformité. Cependant, la complexité de la technologie zk-SNARKs a historiquement posé des défis en termes de mise en œuvre et d'adoption, bien que des améliorations aient été apportées. Les préoccupations réglementaires entourant les cryptomonnaies axées sur la confidentialité peuvent également représenter un défi pour Zcash. Son mécanisme de consensus Proof-of-Work, bien que sécurisé, est plus énergivore que la Preuve d'Enjeu (Proof-of-Stake).

Perspectives : Zcash continue de développer sa technologie pour améliorer l'utilisabilité et l'adoption des transactions chiffrées. L'accent est mis sur l'amélioration de l'expérience utilisateur, l'intégration dans les portefeuilles et les solutions de finance décentralisée (DeFi) privées. Son positionnement en tant que « monnaie numérique » privée et sécurisée, tout en offrant des options de transparence pour la conformité, le positionne comme un acteur pertinent dans l'écosystème crypto pour ceux qui privilégient la confidentialité financière.