ZEC - Zcash

Zcash (ZEC) a été lancé en octobre 2016 par l'Electric Coin Company (ECC), fondée par Zooko Wilcox-O'Hearn, s'appuyant sur des recherches antérieures sur les cryptomonnaies axées sur la vie privée comme Zerocoin et Zerocash. Il s'agit fondamentalement d'un fork de Bitcoin, héritant de son mécanisme de consensus robuste par preuve de travail (PoW) et d'une offre limitée à 21 millions de pièces. Cependant, Zcash se distingue par ses fonctionnalités avancées de confidentialité.

Technologie et confidentialité : L'innovation principale de Zcash réside dans son implémentation des zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). Cette technique cryptographique permet à une partie de prouver la validité d'une transaction sans révéler les données sous-jacentes. Ainsi, les transactions peuvent être vérifiées par le réseau pour s'assurer de l'existence des fonds et de la correction des calculs, sans divulguer l'expéditeur, le destinataire ou le montant.

Zcash utilise un système à double adresse :

- Adresses transparentes (t-adresses) : Elles fonctionnent de manière similaire aux adresses Bitcoin, avec tous les détails de transaction visibles publiquement sur la blockchain.
- Adresses protégées (z-adresses) : Elles exploitent les zk-SNARKs pour chiffrer les détails des transactions, offrant un haut niveau de confidentialité. Les utilisateurs peuvent choisir d'envoyer des transactions entre adresses transparentes et protégées, bien que cela puisse introduire des considérations de confidentialité supplémentaires.

Le réseau utilise l'algorithme Equihash pour le minage, différent du SHA-256 de Bitcoin. Cet algorithme est conçu pour être gourmand en mémoire, visant initialement à égaliser les chances des mineurs, mais conduisant finalement au développement d'ASICs (Application-Specific Integrated Circuits) pour le minage de Zcash.

Tokenomics et offre : La cryptomonnaie native du réseau Zcash est le ZEC. Son offre totale est plafonnée à 21 millions de pièces, reflétant le modèle de rareté de Bitcoin. De nouveaux ZEC sont introduits en circulation par le biais des récompenses de minage. Similairement à Bitcoin, Zcash subit un événement de "halving" environ tous les quatre ans, où la

récompense de bloc est divisée par deux, ralentissant l'émission de nouvelles pièces et contribuant à sa nature déflationniste ou désinflationniste au fil du temps.

Historiquement, les récompenses de bloc ont été partagées entre les mineurs et un fonds de développement. Par exemple, suite à la mise à niveau Canopy, 80% de la subvention de bloc allaient aux mineurs, et 20% finançaient le développement de l'écosystème par le biais d'entités comme l'ECC et la Zcash Foundation. Les événements de halving ultérieurs ont ajusté ces allocations.

Cas d'usage et écosystème : Le ZEC sert de monnaie numérique pour les paiements privés. Ses fonctionnalités de confidentialité le rendent adapté aux utilisateurs et aux entreprises qui nécessitent la confidentialité dans leurs transactions financières. Cela peut inclure :

- Transactions confidentielles : Protection des données financières sensibles contre la vue publique.
- Transferts de fonds : Envoi d'argent à l'international en privé.
- Applications DeFi : Permettre des règlements et des transactions privés au sein des protocoles de finance décentralisée.

L'écosystème Zcash est soutenu par l'Electric Coin Company (ECC), qui dirige le développement principal, et la Zcash Foundation, une organisation à but non lucratif qui promeut le protocole Zcash et son écosystème. Il existe également un réseau de portefeuilles, de clients et de SDK qui prennent en charge les transactions privées.

Gouvernance et développement : Le développement de Zcash est guidé par une double structure impliquant l'ECC et la Zcash Foundation. Cette collaboration assure à la fois l'avancement technique continu du protocole et la promotion de son adoption et de son utilisation plus larges. Le projet a évolué à travers plusieurs mises à niveau réseau, telles que Sapling et Orchard, qui ont amélioré l'efficacité et la convivialité des transactions protégées.

Avantages et limites :

- Avantages :
  - Forte confidentialité : Zcash offre un niveau élevé de confidentialité des transactions grâce aux zk-SNARKs.
  - Transparence optionnelle : Les utilisateurs peuvent choisir leur niveau de confidentialité souhaité, ce qui peut être important pour la conformité

réglementaire.

- Modèle de sécurité de Bitcoin : Construit sur une base de code éprouvée avec une offre plafonnée et un consensus PoW.
- Frais de transaction faibles : Offre généralement des transactions plus rapides et moins chères que Bitcoin.

- Limites :
  - Complexité : La technologie sous-jacente des zk-SNARKs peut être difficile à comprendre.
  - Taille de la blockchain : Historiquement, la blockchain de Zcash a été plus volumineuse que celle d'autres cryptomonnaies en raison des exigences computationnelles des fonctionnalités de confidentialité.
  - Adoption : Bien qu'en croissance, son adoption pour les paiements quotidiens est encore moins répandue que celle des cryptomonnaies plus établies.
  - Surveillance réglementaire : Les cryptomonnaies axées sur la confidentialité peuvent faire l'objet d'une attention réglementaire accrue.

Conclusion : Zcash (ZEC) représente une avancée significative dans le domaine des cryptomonnaies en privilégiant la confidentialité financière des utilisateurs sans sacrifier la sécurité et la vérifiabilité d'une blockchain. Son utilisation innovante des preuves à divulgation nulle de connaissance offre une proposition unique dans le paysage des actifs numériques, attirant les utilisateurs et les institutions recherchant des transactions confidentielles. En maintenant un modèle économique similaire à celui de Bitcoin tout en améliorant la confidentialité, Zcash vise à être une forme d'argent numérique sécurisée, efficace et privée.