# ZEC - Zcash

Zcash (ZEC) est une cryptomonnaie et une blockchain décentralisée conçue pour offrir une confidentialité transactionnelle optionnelle grâce à l'utilisation de la cryptographie avancée. Lancée en octobre 2016 par la Zerocoin Electric Coin Company (aujourd'hui Electric Coin Company - ECC), Zcash est basée sur le code source de Bitcoin mais intègre des innovations majeures pour améliorer la vie privée des utilisateurs.

**Technologie et Fonctionnement :** Le cœur de Zcash réside dans son utilisation des zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Ces preuves cryptographiques permettent de vérifier la validité d'une transaction (par exemple, s'assurer que l'expéditeur dispose des fonds nécessaires et ne dépense pas deux fois les mêmes fonds) sans révéler aucune information sensible telle que l'expéditeur, le destinataire ou le montant de la transaction. Cela rend possible les "transactions blindées", où les détails sont cryptés et privés.

Zcash supporte deux types d'adresses : les adresses transparentes (commençant par 't') qui fonctionnent comme sur Bitcoin et affichent les détails des transactions publiquement, et les adresses blindées (commençant par 'z') qui masquent ces informations. Il est possible de transférer des fonds entre ces deux types d'adresses, offrant une flexibilité aux utilisateurs qui peuvent choisir le niveau de confidentialité souhaité pour chaque transaction.

Les mises à jour récentes, comme le protocole Orchard introduit en 2022, ont encore amélioré les performances et la facilité d'utilisation des transactions blindées, notamment grâce à l'utilisation de la technologie Halo 2 qui a supprimé la nécessité d'une configuration initiale "trusted setup" pour ce système.

**Le Jeton ZEC :** Le ZEC est la monnaie native du réseau Zcash. Il est utilisé pour payer les frais de transaction sur le réseau. Les mineurs, qui sécurisent le réseau par preuve de travail (Proof-of-Work) et utilisent l'algorithme Equihash, sont récompensés en ZEC pour leur contribution.

**Tokenomics :** Zcash partage plusieurs caractéristiques économiques avec Bitcoin. L'offre maximale de ZEC est plafonnée à 21 millions d'unités, ce qui lui confère une certaine rareté. Le réseau connaît des événements de "halving" (division par deux des récompenses de

minage) qui réduisent le rythme d'émission de nouveaux ZEC, comme sur Bitcoin. Par exemple, la deuxième réduction de moitié a eu lieu en novembre 2024, réduisant la subvention de bloc à 1,5625 ZEC.

La répartition de l'allocation initiale comprend une part significative pour la récompense des mineurs (environ 85%), avec des pourcentages dédiés à des entités comme l'Electric Coin Company (ECC), la Zcash Foundation (ZF), des subventions communautaires et un "lockbox" pour le financement du développement et de l'écosystème.

**Cas d'Usage et Utilité :** L'utilité principale de Zcash réside dans sa capacité à faciliter les paiements numériques privés. Cela inclut les transferts personnels discrets, les paiements commerciaux où la confidentialité est cruciale, les dons, et d'autres scénarios où les utilisateurs ne souhaitent pas exposer leurs habitudes de dépenses ou la totalité de leurs avoirs. La fonctionnalité de "divulgation sélective" permet aux utilisateurs de partager des informations de transaction spécifiques avec des auditeurs ou des contreparties autorisées lorsque la transparence est requise, offrant ainsi une solution qui peut potentiellement répondre aux exigences réglementaires tout en préservant la confidentialité.

**Avantages et Limites :** L'avantage majeur de Zcash est son approche optionnelle de la confidentialité, permettant aux utilisateurs de choisir le niveau de discrétion souhaité. Les zk-SNARKs sont une technologie de pointe pour atteindre cet objectif. Cependant, la confidentialité n'est pas automatique ; elle dépend de l'utilisation des adresses blindées et de la compatibilité des portefeuilles et des plateformes avec ces transactions. L'évolutivité et la consommation énergétique du mécanisme de preuve de travail sont également des défis potentiels, bien que des discussions sur l'évolution vers des mécanismes de consensus plus économes en énergie soient en cours.

**Perspectives :** Zcash continue d'évoluer avec des mises à jour visant à améliorer la confidentialité, l'utilisabilité et potentiellement l'évolutivité. L'accent mis sur la vie privée prend de l'importance dans un contexte réglementaire croissant et une adoption institutionnelle plus large des cryptomonnaies, positionnant Zcash comme une option pour ceux qui recherchent des transactions numériques plus confidentielles. L'amélioration de l'expérience utilisateur (UX), notamment à travers des portefeuilles comme Zashi, vise à réduire les frictions pour l'utilisation des transactions blindées.