

NIGHT - Midnight

Le Midnight Network est une blockchain de quatrième génération conçue pour offrir une "vie privée rationnelle", permettant de concilier utilité et protection des données.

Développé avec des liens étroits avec l'écosystème Cardano, Midnight utilise des preuves à divulgation nulle de connaissance (ZKP) pour construire des applications décentralisées (dApps) qui garantissent la confidentialité des données des utilisateurs, des transactions commerciales et des métadonnées, tout en permettant la vérification de la validité des informations. La technologie ZKP est au cœur du réseau, permettant des opérations à la fois transparentes et privées sur la même chaîne.

Le token NIGHT est l'actif natif et non protégé (unshielded) du Midnight Network. Son rôle principal est d'assurer la sécurité du réseau et de générer le DUST, une ressource protégée (shielded) et non transférable indispensable pour effectuer des transactions et exécuter des contrats intelligents sur le réseau. Ce modèle de "token génère ressource" est une innovation clé : détenir du NIGHT permet de produire continuellement du DUST, qui est consommé lors des transactions. Une fois consommé, le DUST se régénère avec le temps en fonction des avoirs en NIGHT, créant ainsi un système de ressources renouvelables. Cette approche découple le coût des opérations de la valeur du token NIGHT, offrant une prévisibilité des coûts pour les entreprises et les utilisateurs réguliers, et évitant la nécessité de dépenser constamment le NIGHT lui-même pour les frais de transaction. Le NIGHT est également le token de gouvernance, donnant à ses détenteurs le droit de voter sur les propositions d'évolution du réseau.

La tokenomie de Midnight est conçue pour être coopérative et interopérable, visant à étendre l'accès au réseau et à faciliter la création de valeur inter-chaînes. Des mécanismes comme le "sponsored access" permettent aux DApps de prendre en charge les frais de DUST pour leurs utilisateurs, rendant l'interaction avec l'application gratuite pour l'utilisateur final. Des marchés de capacité futurs sont envisagés pour permettre la location de génération de DUST.

La sécurité du réseau est assurée par un mécanisme d'incitation aux producteurs de blocs (validateurs). Les opérateurs de pools de staking Cardano (SPOs) peuvent agir en tant que validateurs et être récompensés en NIGHT pour la sécurisation de la chaîne. La structure de

récompense des validateurs et le financement du développement futur du réseau sont gérés par une Réserve (Reserve) et un Trésorier (Treasury) intégrés.

Concernant la distribution du token NIGHT, un effort particulier a été fait pour garantir un lancement équitable et décentralisé. Le processus a débuté par des phases comme le "Glacier Drop" et le "Scavenger Mine", visant à permettre à un large public de réclamer des tokens sans coût initial. L'offre totale de NIGHT est fixe à 24 milliards de tokens, créés dès le départ mais pas nécessairement tous en circulation immédiatement. La distribution vise à une possession décentralisée sans allocation pré-allouée pour l'équipe ou les investisseurs au lancement.

Les avantages du Midnight Network incluent la confidentialité par défaut, des coûts opérationnels prévisibles, une intégration facilitée pour les développeurs grâce à un langage de contrat intelligent basé sur TypeScript (Compact), et un potentiel d'adoption élevé pour des applications axées sur la confidentialité dans des domaines tels que la finance décentralisée (DeFi), la gestion d'identité, et l'intelligence artificielle.

Cependant, le projet fait face à des limites potentielles liées à l'adoption de nouvelles technologies de confidentialité, à la concurrence dans l'espace blockchain, et à la nécessité d'une adoption significative par les développeurs et les utilisateurs pour réaliser son plein potentiel. Les perspectives du projet reposent sur son succès à équilibrer vie privée et conformité réglementaire, à attirer une communauté active de développeurs, et à s'établir comme une infrastructure clé pour les applications nécessitant une confidentialité programmable et vérifiable.