RAIL - Railgun

Le token RAIL est intrinsèquement lié au protocole Railgun, une solution de confidentialité construite sur la blockchain Ethereum qui s'étend à d'autres réseaux compatibles EVM tels que le BNB Smart Chain (BSC), Polygon et Arbitrum. L'objectif fondamental de Railgun est d'introduire la confidentialité dans l'écosystème DeFi, qui est par nature transparent. Il y parvient en utilisant des preuves Zero-Knowledge (ZK), spécifiquement les ZK-SNARKs, pour anonymiser les transactions sans compromettre leur validité vérifiable par la blockchain.

L'utilité principale du token RAIL est la gouvernance du protocole. Les détenteurs de RAIL peuvent staker leurs tokens pour obtenir des droits de vote sur les propositions d'améliorations ou de modifications du protocole. Ce mécanisme vise à décentraliser la prise de décision, garantissant qu'aucun privilège spécial ne soit accordé aux développeurs du projet par rapport aux détenteurs du token. De plus, le staking de RAIL peut également donner accès à des récompenses de sécurité et des incitations du trésor pour les participants actifs à la gouvernance.

Sur le plan technique, Railgun fonctionne comme un système de contrats intelligents directement sur la chaîne (on-chain), éliminant le besoin de ponts inter-chaînes ou de solutions de couche 2 (Layer-2) qui pourraient introduire des vulnérabilités de sécurité ou fragmenter la liquidité. Il permet aux utilisateurs de "shielder" (masquer) leurs actifs dans des adresses privées, d'effectuer des transactions anonymes et d'interagir avec diverses applications décentralisées (dApps) tout en préservant la confidentialité des détails de la transaction tels que l'expéditeur, le destinataire, le type d'actif et le montant. L'expérience utilisateur est conçue pour être similaire à celle d'un portefeuille public standard, mais avec la capacité d'opérer en privé.

Le token RAIL est un token ERC-20 standard et est disponible sur les échanges décentralisés comme SushiSwap et Uniswap. L'offre maximale de tokens RAIL sur Ethereum est de 100 millions. Cependant, il est important de noter que Railgun a également déployé des tokens de gouvernance spécifiques pour ses instances sur le BNB Smart Chain (RAILBSC) et Polygon (RAILPOLY), avec des offres maximales distinctes. Ces tokens ont été distribués via des airdrops aux stakers de RAIL et aux fournisseurs de liquidité sur ces

chaînes respectives.

Il est crucial de comprendre que la détention de tokens RAIL n'est pas une condition préalable à l'utilisation du système de confidentialité de Railgun, et elle ne confère pas elle-même de confidentialité. Son rôle est strictement lié à la gouvernance et à la sécurité du protocole. Railgun se positionne comme une "couche de confidentialité universelle" pour la DeFi, offrant une solution non fiduciaire et entièrement intégrée qui vise à rendre la DeFi accessible à un public plus large en résolvant le compromis actuel entre transparence et confidentialité. Les avantages pour l'utilisateur incluent la protection contre les acteurs malveillants et la possibilité de protéger des stratégies de trading confidentielles ('alpha protection'). Le projet met l'accent sur la sécurité, avec des audits réalisés par des firmes réputées.