# RAIL - Railgun

Railgun est un système de confidentialité conçu pour apporter l'anonymat aux transactions sur les blockchains publiques.

**Fonctionnement et Technologie** Le protocole utilise la cryptographie à divulgation nulle, plus spécifiquement les preuves ZK-SNARKs, pour anonymiser les interactions des utilisateurs avec les contrats intelligents et les applications DeFi. Cela signifie que les utilisateurs peuvent échanger, prêter, ajouter de la liquidité ou utiliser des dApps sans que leurs adresses de portefeuille et l'historique de leurs transactions ne soient rendus publics. Railgun fonctionne directement sur la chaîne (on-chain) sur des blockchains telles qu'Ethereum, Polygon, BNB Smart Chain et Arbitrum, éliminant ainsi le besoin de solutions de couche 2 ou de ponts entre chaînes, considérés comme des points de vulnérabilité potentiels. Les transactions sont traitées via des contrats intelligents qui vérifient leur validité sans révéler les détails sous-jacents.

**Cas d'Usage et Utilité** L'objectif principal de Railgun est de permettre aux utilisateurs de DeFi de maintenir leur vie privée. Cela est particulièrement utile pour les traders professionnels qui souhaitent protéger leurs stratégies de trading, les entreprises qui doivent respecter la confidentialité financière, ou tout utilisateur désireux de garder ses activités financières privées. Railgun permet aux utilisateurs d'interagir avec divers protocoles DeFi, y compris les échanges décentralisés (DEXs) et les plateformes de prêt, tout en bénéficiant d'une confidentialité totale. Les utilisateurs peuvent constituer des soldes privés et effectuer des transactions sans avoir à retirer leurs fonds de leur portefeuille privé vers un portefeuille public.

**Le Token RAIL** Le token RAIL est le token de gouvernance natif du protocole Railgun. Il permet aux détenteurs de participer au processus de gouvernance décentralisée (DAO), en votant sur les propositions de mise à niveau et les modifications du protocole. Pour participer au vote, les détenteurs de RAIL doivent staker leurs tokens, selon le principe d'un token, une voix. Il existe des tokens spécifiques pour chaque blockchain prise en charge : RAIL sur Ethereum, RAILPOLY sur Polygon et RAILBSC sur BNB Smart Chain, chacun gouvernant le déploiement de Railgun sur sa chaîne respective. Ces tokens (RAILPOLY et RAILBSC) ont été distribués via des airdrops aux stakers et aux fournisseurs de liquidité de

RAIL.

**Tokenomics et Distribution** La fourniture maximale de tokens varie selon la chaîne : 100 millions de RAIL sur Ethereum, 55 millions de RAILPOLY sur Polygon et environ 44,5 millions de RAILBSC sur BNB Smart Chain. Le projet est structuré de manière décentralisée, sans investisseurs en capital-risque ni détenteurs d'actions. Une partie des tokens est allouée à la DAO, qui peut les émettre via un vote pour récompenser les développeurs ou promouvoir la plateforme. La distribution des tokens RAILPOLY et RAILBSC s'est notamment faite par le biais d'airdrops pour encourager la participation précoce et la liquidité.

**Avantages et Limites** Les principaux avantages de Railgun résident dans sa forte confidentialité, sa décentralisation et sa sécurité grâce à l'utilisation des preuves à divulgation nulle et à son fonctionnement on-chain. En évitant les ponts et les solutions de couche 2, il réduit les risques de sécurité. Sa compatibilité avec n'importe quelle application décentralisée sur Ethereum et d'autres blockchains compatibles EVM est un atout majeur. Cependant, la complexité technologique des preuves à divulgation nulle peut constituer une barrière à l'adoption pour certains utilisateurs, bien que les interfaces frontales visent à simplifier l'expérience. Le fait qu'il ne s'agisse pas d'une monnaie de confidentialité mais d'un protocole de confidentialité est également une distinction importante.

**Perspectives** Railgun vise à devenir la solution de confidentialité de référence pour la DeFi, offrant de nouvelles possibilités commerciales et une plus grande liberté financière aux utilisateurs. Le développement de fonctionnalités comme le portefeuille multisignature privé montre l'engagement de l'équipe à innover et à répondre aux besoins des utilisateurs en matière de sécurité et de confidentialité, attirant l'attention de personnalités comme Vitalik Buterin, co-fondateur d'Ethereum.