ZERA - ZERA

ZERA est le jeton utilitaire du protocole Zera Labs, une plateforme qui vise à introduire des fonctionnalités de confidentialité avancées pour les actifs numériques existants. Construit initialement sur la blockchain Solana, ZERA utilise des technologies cryptographiques, notamment les preuves à divulgation nulle de connaissances (zero-knowledge proofs ou ZKPs), pour permettre des transactions privées et sécurisées. L'objectif principal est de transformer des crypto-actifs comme l'USDC, l'USDT, ou le SOL en une forme de "monnaie numérique" qui offre une confidentialité similaire à celle de l'argent liquide, mais avec les avantages du numérique.

Le fonctionnement repose sur un système de "notes cryptographiques". Les utilisateurs déposent leurs actifs pris en charge dans le protocole, et en retour, ils reçoivent ces notes. Ces notes peuvent ensuite être utilisées pour des transferts privés et confidentiels, même hors ligne, en utilisant des technologies comme le NFC, le Bluetooth ou les codes QR. La technologie ZK assure que la validité des transactions est vérifiée sans révéler les détails sensibles tels que l'expéditeur, le destinataire ou le montant. Cela est rendu possible grâce à des primitives cryptographiques telles que les engagements Pedersen et les nullificateurs, qui empêchent les doubles dépenses tout en préservant la confidentialité.

Le token ZERA joue un rôle central dans l'écosystème. Il est utilisé pour la gouvernance du protocole, permettant aux détenteurs de participer aux décisions relatives à son développement. Il offre également un accès à des fonctionnalités premium au sein de la plateforme et est conçu pour avoir une utilité économique à travers des mécanismes de rachat et de destruction programmatiques. Ces derniers lient la réduction de l'offre du token à l'utilisation du protocole, créant ainsi un modèle de valeur axé sur l'adoption et l'activité réseau, sans imposer de frais directs sur les transactions privées. L'objectif est de créer un effet de levier où une utilisation accrue du protocole entraîne une diminution de l'offre de tokens, renforçant potentiellement sa valeur.

L'un des aspects distinctifs de ZERA est sa conception "agnostique d'actifs". Cela signifie qu'il peut fonctionner avec divers stablecoins et tokens existants sans nécessiter de mécanismes de wrapping (enveloppement) ou des pools de liquidité spécifiques à chaque actif. Il tire parti d'un "pool ZK unifié", créant une seule chambre d'anonymat pour plusieurs

actifs, ce qui améliore la confidentialité par rapport aux systèmes qui maintiennent des pools séparés. La plateforme est également conçue pour être non-custodiale, ce qui signifie qu'elle ne détient pas directement les actifs des utilisateurs, privilégiant la compatibilité avec les portefeuilles et les applications décentralisées (dApps) existants.

Les avantages de ZERA incluent la confidentialité renforcée pour les transactions, la possibilité de paiements hors ligne, la compatibilité avec les actifs existants et la rapidité des transactions grâce à la blockchain Solana. Les limites potentielles pourraient inclure la complexité technologique inhérente aux preuves à divulgation nulle de connaissances, la dépendance à l'égard de l'adoption par les utilisateurs et les défis réglementaires liés aux transactions privées.

En résumé, ZERA se positionne comme une solution innovante pour apporter la confidentialité des paiements numériques, similaire à celle de l'argent physique, tout en s'intégrant dans l'écosystème DeFi existant. Son approche axée sur l'utilité du token et les mécanismes de déflation par l'usage le distingue dans le paysage des cryptomonnaies axées sur la confidentialité.