LA - Lagrange

Lagrange se positionne comme une infrastructure clé pour la vérification cryptographique dans les domaines de l'IA et de la blockchain. Le projet repose sur trois piliers technologiques principaux : le Réseau de Prouveurs ZK (ZK Prover Network), le Coprocesseur ZK (ZK Coprocessor) et DeepProve.

Le Réseau de Prouveurs ZK est un réseau décentralisé d'opérateurs capables de générer des preuves à connaissance nulle (ZKP) à la demande. Lorsqu'une application décentralisée (dApp) a besoin de prouver la validité d'un calcul effectué hors chaîne, elle soumet une requête à Lagrange. Le réseau s'occupe alors des calculs complexes et renvoie une preuve compacte que les smart contracts peuvent vérifier. Ce réseau fonctionne sur EigenLayer et est soutenu par de nombreux opérateurs, garantissant la disponibilité et la fiabilité des preuves.

Le Coprocesseur ZK est conçu comme un moteur de requête sans confiance pour les données blockchain. Il permet aux développeurs d'écrire des requêtes SQL pour extraire des données de milliers de blocs, d'effectuer des calculs tels que des moyennes ou des sommes, et d'obtenir une ZKP. Cette preuve peut ensuite être intégrée directement dans un smart contract pour vérification. Cela ouvre la voie à des calculs complexes et à des requêtes de données sur plusieurs chaînes sans nécessiter de ponts.

DeepProve est une bibliothèque zkML (machine learning avec connaissance nulle) qui permet la vérification cryptographique des inférences d'IA. Elle garantit que les résultats de l'IA sont corrects et qu'ils proviennent du modèle attendu, sans révéler les données d'entrée. DeepProve est présenté comme étant significativement plus rapide que les solutions zkML existantes et vise à rendre l'IA plus fiable et transparente dans des domaines critiques comme la santé, les systèmes autonomes et les services financiers.

Le token LA est le token utilitaire natif de l'écosystème Lagrange. Son utilité est multiple : il est utilisé par les clients pour payer les frais de génération de preuves, ce qui aligne la demande de token sur la demande de preuves cryptographiques. Il sert également à récompenser les opérateurs du réseau de prouveurs, les incitant à maintenir la fiabilité du réseau. De plus, les détenteurs de tokens LA peuvent les staker ou les déléguer à des prouveurs spécifiques, renforçant ainsi la sécurité et la décentralisation du réseau. Les

tokenomics de LA sont conçues autour du principe que la demande de preuve génère directement la demande de token.

Les cas d'usage de Lagrange incluent l'amélioration de la scalabilité des ZK rollups, la vérification des données entre différentes blockchains, l'exécution de calculs complexes pour les smart contracts, et surtout, la vérification de l'IA pour garantir la fiabilité et la confidentialité des modèles d'intelligence artificielle. Le projet vise à devenir une infrastructure fondamentale pour l'internet vérifiable, où la confiance est remplacée par la certitude mathématique grâce aux preuves cryptographiques.