ZANO - Zano

ZANO est une plateforme blockchain de couche 1, open-source, conçue pour offrir un haut niveau de confidentialité, de sécurité et de scalabilité. Lancé en 2019, le projet se distingue par son approche "privacy-by-default", où toutes les transactions masquent par défaut l'identité de l'expéditeur et du destinataire, le montant de la transaction, et même le type d'actif échangé. Cette confidentialité est assurée par des technologies cryptographiques avancées, notamment les signatures d'anneau (ring signatures), les adresses furtives (stealth addresses) et les engagements de Pedersen avec Bulletproofs+ pour les montants.

Au cœur de ZANO se trouve un mécanisme de consensus hybride combinant Proof-of-Work (PoW) et Proof-of-Stake (PoS). Cette approche vise à renforcer la sécurité en rendant les attaques telles que la double dépense coûteuses et improbables. Une innovation notable est le premier système Proof-of-Stake privé (Zarcanum protocol), qui permet aux utilisateurs de staker leurs ZANO sans révéler leurs avoirs ou transactions sur la chaîne, tout en maintenant la sécurité du réseau.

L'utilité du token ZANO est multiple. Il sert de carburant pour les frais de transaction sur le réseau, quelle que soit l'opération (envoi de ZANO, enregistrement d'alias, émission d'actifs confidentiels). Il est également utilisé pour récompenser les mineurs et les stakers qui contribuent à la sécurité du réseau.

ZANO se positionne non seulement comme une monnaie axée sur la confidentialité, mais aussi comme une plateforme pour la création d'actifs confidentiels (Confidential Assets). Cela permet aux développeurs d'émettre leurs propres tokens privés (stablecoins, NFTs, tokens de gouvernance) sur la blockchain ZANO, héritant ainsi des caractéristiques de confidentialité du protocole. L'écosystème ZANO comprend également des applications comme Zano Trade, un échange décentralisé basé sur les Ionic Swaps, et des API pour construire des marchés décentralisés. Des projets tels que Confidential Layer pour la confidentialité inter-chaînes, le stablecoin privé Freedom Dollar, et la plateforme NFT privée Obscura sont en développement.

L'économie du token (tokenomics) de ZANO est caractérisée par une politique monétaire simple : une émission fixe par bloc (1 ZANO) et une combustion de 100% des frais de transaction. Il n'y a pas de maximum d'offre prédéfini, mais l'inflation est compensée par la

combustion des frais, ce qui peut potentiellement mener à une déflation si l'utilisation de la chaîne est suffisamment élevée. Le projet a mis en place une pré-mine initiale pour couvrir les dépenses de développement et de marketing, dont une partie importante a déjà été dépensée, contribuant à la décentralisation progressive.

Les cas d'usage de ZANO incluent les paiements privés et sécurisés, le staking privé, la création d'actifs confidentiels, et potentiellement des applications comme des contrats d'entiercement (escrow) pour l'e-commerce privé et des échanges décentralisés sans inscription. La fonctionnalité Zano Alias vise également à simplifier l'interaction avec l'écosystème en permettant la création d'identifiants uniques.

Cependant, la nature "privacy-by-default" de ZANO présente également des défis, notamment en matière de conformité réglementaire et d'intégration avec les intermédiaires centralisés comme les bourses. L'absence de "compliance by analytics" rend plus complexe l'auditabilité des transactions pour les tiers. La gouvernance du projet est également présentée comme plus centralisée, avec un système de vote axé sur les signaux communautaires pour les aspects de l'écosystème, plutôt que sur le contrôle du protocole technique.