

ZANO - Zano

ZANO est une plateforme blockchain de couche 1, open-source, qui met l'accent sur la confidentialité, la sécurité et la scalabilité, conçue pour être une base robuste pour les actifs confidentiels et les applications décentralisées (dApps). Son objectif principal est d'offrir des transactions privées par défaut, où les détails tels que l'expéditeur, le destinataire, le montant et le type d'actif sont masqués pour tous les participants.

La technologie de confidentialité de ZANO repose sur une combinaison de signatures de cercle (ring signatures), d'adresses furtives (stealth addresses) et de Bulletproofs+. Les signatures de cercle permettent de mélanger les transactions réelles avec des transactions fictives pour masquer l'origine. Les adresses furtives assurent que les destinataires ne peuvent être retracés. Les Bulletproofs+ sont utilisés pour masquer les montants des transactions tout en assurant l'auditabilité de l'offre globale. ZANO a également été développé à partir du code original du protocole CryptoNote, la technologie de confidentialité qui alimente d'autres cryptomonnaies comme Monero.

Le mécanisme de consensus de ZANO est un hybride Proof-of-Work (PoW) et Proof-of-Stake (PoS). Le PoW sécurise le réseau grâce à la puissance de calcul GPU, tandis que le PoS incite à un alignement entre l'investissement en capital et la sécurité du réseau. Une innovation clé est le protocole Zarcum, qui est le premier mécanisme de Proof-of-Stake à dissimuler les montants de staking, renforçant ainsi la confidentialité même lors de la participation au consensus. Cette approche hybride vise à rendre les attaques sur le réseau extrêmement coûteuses.

Au-delà des transactions confidentielles, ZANO prend en charge les "Confidential Assets", permettant aux utilisateurs de créer leurs propres jetons privés sur la blockchain ZANO. Ces actifs héritent des mêmes caractéristiques de confidentialité que le token natif ZANO. Cela ouvre la voie à la création de stablecoins privés, de versions sécurisées d'actifs existants, et d'autres tokens personnalisés sans nécessiter de gérer sa propre blockchain.

L'écosystème ZANO est conçu pour prendre en charge diverses applications décentralisées (dApps) et cas d'usage. Il comprend des fonctionnalités telles que les "Ionic Swaps" pour des échanges atomiques (atomic swaps) sans confiance et privés, un marché décentralisé (DEX) appelé Zano Trade, et des "Aliases" qui fournissent des identifiants humains lisibles et

sécurisés (par exemple, @nomdutilisateur) pour simplifier les interactions et l'identité sur le réseau. Les "Escrow Trades" permettent des échanges d'actifs conditionnels et sans intermédiaire, utiles pour les plateformes de commerce électronique décentralisées et le trading peer-to-peer. Des "Auditable Wallets" optionnels permettent également une transparence pour des cas d'usage spécifiques, comme la gestion des fonds de développement, sans compromettre la confidentialité du réseau.

Le token ZANO est la cryptomonnaie native de la blockchain. Il est utilisé pour alimenter les transactions, sécuriser le réseau via le staking, enregistrer des Aliases, et participer à la gouvernance du réseau par le biais d'un système de vote. La tokenomie de ZANO prévoit que tous les frais de réseau sont brûlés ("burned"). Combiné à des émissions de blocs relativement basses, cela peut potentiellement conduire à une offre déflationniste à long terme si l'utilisation du réseau est suffisamment élevée. L'offre maximale de ZANO n'est pas strictement plafonnée, mais l'offre en circulation est d'environ 15 millions de tokens.

En résumé, ZANO se positionne comme une infrastructure axée sur la confidentialité pour la finance décentralisée et la propriété d'actifs, répondant à une demande croissante pour des transactions résistantes à la censure. Sa technologie hybride, son écosystème en expansion et son accent sur la confidentialité en font une proposition intéressante pour les utilisateurs et les développeurs recherchant des solutions décentralisées et privées.