

ZANO - Zano

Zano se présente comme un écosystème de blockchain de couche 1 axé sur la confidentialité, construit à partir des bases du protocole CryptoNote, qui est à l'origine de monnaies axées sur la confidentialité comme Monero. Lancé en 2019, Zano vise à offrir une solution complète pour les transactions financières privées, les actifs numériques et les marchés décentralisés, en mettant l'accent sur la sécurité, la scalabilité et la confidentialité par défaut.

Confidentialité par Défaut et Technologies Cryptographiques

Le cœur de Zano réside dans son architecture de confidentialité par défaut. Chaque transaction sur le réseau masque automatiquement des informations cruciales : l'expéditeur, le destinataire, le montant et le type d'actif. Ceci est rendu possible par l'utilisation combinée de plusieurs techniques cryptographiques avancées :

- **Signatures d'anneau (Ring Signatures)** : Elles mélangent l'expéditeur réel avec plusieurs transactions similaires, rendant l'origine de la transaction intraquable.
- **Adresses furtives (Stealth Addresses)** : Des adresses uniques à usage unique sont générées pour chaque transaction, rompant le lien entre le destinataire et ses adresses publiques.
- **Engagements de Pedersen et Bulletproofs+ (Pedersen Commitments & Zero-Knowledge Bulletproofs+)** : Ces méthodes permettent de masquer les montants des transactions tout en assurant que l'offre totale reste vérifiable, garantissant la confidentialité des montants sans compromettre l'auditabilité.

Mécanisme de Consensus Hybride : Preuve de Travail (PoW) et Preuve de Participation (PoS) Privée

Zano utilise un mécanisme de consensus hybride unique qui combine la Preuve de Travail (PoW) et une forme innovante de Preuve de Participation (PoS) appelée Zarcantum. Le PoW sécurise le réseau grâce au minage, tandis que le PoS Zarcantum permet aux détenteurs de ZANO de staker leurs jetons pour sécuriser le réseau et gagner des récompenses, tout en préservant la confidentialité de leurs soldes. Cette approche hybride vise à maximiser la sécurité, la décentralisation et l'efficacité énergétique, tout en rendant les attaques sur le

réseau plus coûteuses.

Actifs Confidentiels et Écosystème Décentralisé

Au-delà des transactions privées, Zano fonctionne comme une plateforme pour une économie numérique privée. Une caractéristique clé est la prise en charge des **Actifs Confidentiels (Confidential Assets)**. Cette fonctionnalité permet à quiconque de créer et d'émettre ses propres jetons privés sur la blockchain Zano. Ces jetons héritent des mêmes caractéristiques de confidentialité que le ZANO natif, ce qui signifie que leurs montants et types d'actifs peuvent également être cachés. Cela ouvre la voie à la création de :

- Stablecoins privés.
- Versions privées d'actifs existants (par exemple, des actions tokenisées ou des devises).
- Jetons de gouvernance privés.
- NFTs axés sur la confidentialité.

L'écosystème Zano comprend également des projets tels que :

- **Zano Trade** : Un échange décentralisé (DEX) natif permettant des échanges atomiques sans confiance.
- **Pont Confidential Layer** : Permet le transfert d'actifs privés entre Zano et d'autres blockchains comme Bitcoin et Ethereum.
- **Freedom Dollar** : Un exemple de stablecoin privé émis sur Zano.
- **Places de marché privées** et autres applications décentralisées (dApps) conçues pour fonctionner dans un environnement de confidentialité.

Le Token ZANO

Le ZANO est la cryptomonnaie native de l'écosystème. Il joue plusieurs rôles essentiels :

- **Frais de Transaction** : Chaque transaction effectuée sur la blockchain Zano, qu'il s'agisse d'envoyer des ZANO, d'enregistrer un alias ou d'émettre un actif privé, utilise ZANO comme monnaie pour les frais.
- **Staking** : Les détenteurs de ZANO peuvent staker leurs jetons pour contribuer à la sécurité du réseau et recevoir des récompenses, tout en bénéficiant de la confidentialité de leurs soldes.
- **Gouvernance** : Le token peut être utilisé pour la gouvernance, permettant aux

détenteurs de voter anonymement sur le développement futur du protocole.

- **Alimentation de l'Écosystème** : Il sert de monnaie principale pour interagir avec les diverses applications et services construits sur la plateforme Zano.

Une caractéristique notable de la tokenomie de ZANO est la **brûlure de tous les frais de transaction**. Avec une utilisation suffisante du réseau, la quantité de ZANO brûlée quotidiennement pourrait surpasser l'émission des récompenses de bloc, rendant ainsi l'offre déflationniste à terme. Cette combinaison d'émissions faibles et de brûlures de frais réduit la pression de vente potentielle sur les marchés.

Cas d'Usage et Avantages Potentiels

Zano offre une proposition de valeur claire pour les utilisateurs et développeurs valorisant la confidentialité :

- **Transactions Privées** : Idéal pour ceux qui recherchent l'anonymat financier, que ce soit pour des raisons personnelles ou professionnelles.
- **Développement de dApps Privées** : Fournit une infrastructure pour créer des applications décentralisées où la confidentialité des données est primordiale.
- **Gestion d'Actifs Confidentiels** : Permet la création et la gestion d'actifs numériques privés sur mesure.
- **Usabilité Améliorée avec Zano Alias** : La fonctionnalité Zano Alias simplifie les interactions avec l'écosystème en associant des noms lisibles par l'homme à des adresses de paiement, ce qui est une étape vers une adoption plus large.
- **Marchés Résistants à la Censure** : La nature privée des transactions rend l'écosystème plus résistant à la censure.

Limites et Perspectives

Bien que Zano offre des fonctionnalités de confidentialité avancées, comme pour de nombreux projets axés sur la vie privée, il peut faire face à des défis liés à la complexité de la technologie, à la perception du public, à l'adoption par les développeurs et à la conformité réglementaire potentielle. Cependant, en se concentrant sur une confidentialité robuste par défaut, un écosystème en croissance et des innovations continues comme le PoS privé, Zano se positionne comme une plateforme prometteuse pour l'avenir de la finance numérique privée. L'intégration avec des services comme AEON Pay pour des paiements dans le monde réel élargit encore son utilité potentielle.