

ZBT - ZEROBASE

ZEROBASE est une plateforme d'infrastructure décentralisée qui fournit la génération de preuves à divulgation nulle de connaissance (ZKPs) en temps réel, visant à améliorer la confidentialité, la confiance et la transparence dans les applications blockchain.

Fonctionnement et Technologie : ZEROBASE combine les ZKPs avec des environnements d'exécution de confiance (TEEs). Les ZKPs permettent de prouver la véracité d'une déclaration sans révéler les informations sous-jacentes, tandis que les TEEs offrent un environnement matériel sécurisé pour le traitement des données sensibles. Cette combinaison permet des calculs hors chaîne qui sont à la fois privés et vérifiables sur la chaîne.

Le réseau est structuré autour d'un système à deux niveaux de nœuds : les HUB Nodes qui routent les tâches et gèrent la bande passante, et les Proving Nodes qui génèrent les preuves ZK dans des TEEs sécurisés. Cette architecture vise à assurer une distribution efficace de la charge, la scalabilité, la tolérance aux pannes et des incitations économiques pour la performance et la sécurité. ZEROBASE est déployé sur les blockchains compatibles EVM, notamment Ethereum, Arbitrum, Optimism, Base, Polygon, Avalanche et BNB Chain, avec une compatibilité omnichain via le standard OFT de LayerZero.

Utilité et Cas d'Usage : Le token ZBT est au cœur de l'écosystème ZEROBASE. Il est utilisé pour payer les services du réseau, tels que la génération et le routage de preuves, et pour inciter les opérateurs de nœuds à maintenir la sécurité et la performance du réseau. Les détenteurs de ZBT peuvent également participer aux processus de gouvernance, y compris la proposition et le vote sur les paramètres du réseau.

Les applications clés de ZEROBASE incluent :

- **zkLogin** : Authentification préservant la vie privée en utilisant des identifiants existants (par exemple, Google) sans révéler d'informations personnelles sensibles.
- **zkStaking** : Permet de générer des rendements sur les actifs tout en maintenant la confidentialité des stratégies de staking et en assurant la transparence des risques.
- **zkAuditing** : Fournit des preuves de conformité pour les audits d'entreprise, permettant de vérifier les transactions sans exposer les détails sensibles.

- **zkDarkPool** : Facilite les transactions confidentielles sur les échanges décentralisés.

Tokenomics : Le ZBT a une offre totale fixe d'un milliard de tokens. La répartition comprend des allocations pour l'équipe et les conseillers (20%), les investisseurs (11.25%), la liquidité (2%), un fonds de croissance (15%), des airdrops et les premiers mineurs (8%), et une part importante pour les récompenses de staking des nœuds (43.75%). Le projet met l'accent sur l'utilité du token comme instrument d'accès aux services du réseau et de gouvernance, et non comme instrument d'investissement spéculatif.

Avantages et Limites : Les avantages de ZEROBASE résident dans sa capacité à offrir des solutions de confidentialité et de scalabilité pour des applications complexes, notamment dans le domaine financier, tout en respectant les exigences réglementaires. La génération de preuves en millisecondes à un coût inférieur à un centime est également un avantage notable. Cependant, l'adoption de technologies ZK et TEE avancées peut présenter des défis en termes de complexité technique et d'adoption par le grand public et les institutions.

Perspectives : Fondé en mars 2024 par Mirror Tang, un professeur de cryptographie, ZEROBASE a levé 5 millions de dollars auprès d'investisseurs de premier plan tels que Binance Labs, Lightspeed Faction et Sequoia Capital. Le projet se positionne comme un pont entre la finance traditionnelle et la blockchain, en exploitant la puissance des preuves à divulgation nulle de connaissance pour un avenir financier plus privé et vérifiable.