

AZTEC - Aztec

Aztec Network se positionne comme une infrastructure essentielle pour le Web3 en s'attaquant au problème de la transparence forcée inhérente aux blockchains publiques, notamment Ethereum. Il s'agit d'une solution de couche 2 (L2) qui exploite les preuves à divulgation nulle de connaissance (zero-knowledge proofs) pour offrir une confidentialité programmable.

Technologie et Fonctionnement Aztec fonctionne comme un zk-rollup (Zero-Knowledge Rollup). Les zk-rollups sont des solutions L2 qui traitent les transactions en dehors de la chaîne principale d'Ethereum (off-chain) mais soumettent des preuves cryptographiques à la chaîne principale (on-chain) pour validation. Cela permet d'augmenter la scalabilité (plus de transactions par seconde) et de réduire les coûts de transaction par rapport à la chaîne principale d'Ethereum. Ce qui distingue Aztec est son architecture axée sur la confidentialité. Il utilise un modèle d'exécution hybride comprenant un Environnement d'Exécution Privé (PXE) où les calculs privés s'effectuent localement sur les appareils des utilisateurs, et une Machine Virtuelle Aztec (AVM) pour la logique publique. Ce système permet aux développeurs de créer des applications où les données sensibles (montants de transaction, soldes, stratégies de trading, etc.) restent cryptées, tout en assurant la vérifiabilité publique des résultats finaux. Le réseau est construit autour de Noir, un langage de programmation conçu pour la logique cryptographique, facilitant le développement d'applications combinant des éléments privés et publics.

Token AZTEC Le token AZTEC est le jeton utilitaire natif du réseau Aztec. Son offre maximale est fixée à 10,35 milliards de tokens. Les fonctions principales du token AZTEC incluent :

- **Sécurité du Réseau (Staking)** : Les validateurs (Sequencers) doivent staker des tokens AZTEC comme garantie pour participer à la production de blocs. Cela sécurise le réseau et aligne les incitations. Des mécanismes comme le slashing (réduction de la mise) sont en place pour décourager les comportements malveillants.
- **Gouvernance** : Les détenteurs de tokens AZTEC ont un rôle dans la gouvernance du protocole, leur permettant de voter sur les mises à jour et les décisions importantes du réseau.

- **Frais de Transaction** : Le token AZTEC peut être utilisé pour payer les frais de gaz sur le réseau Aztec. Le système de frais est adaptatif, potentiellement déflationniste en période de forte congestion (les frais excédentaires étant brûlés) et inflationniste avec des récompenses pour les séquenceurs et les validateurs en période de faible utilisation.

La distribution du token AZTEC est structurée pour équilibrer la croissance de l'écosystème, la compensation de l'équipe et la participation communautaire, avec des allocations pour la vente publique, les subventions à l'écosystème, les incitations futures et les récompenses réseau.

Cas d'Usage et Avantages Aztec Network ouvre la voie à plusieurs cas d'utilisation innovants qui étaient auparavant impossibles sur des blockchains publiques en raison des problèmes de confidentialité :

- **Finance Décentralisée (DeFi) Privée** : Permet des swaps, des prêts, des emprunts et du staking sans révéler les montants, les stratégies ou les positions. Cela protège les stratégies de trading et améliore la sécurité des utilisateurs.
- **Applications d'Entreprise** : Les entreprises peuvent exécuter des opérations de trésorerie privées, des chaînes d'approvisionnement confidentielles, des paiements B2B et des pistes d'audit conformes sans exposer de données sensibles à leurs concurrents ou au public.
- **Identité Privée** : Utilisation des preuves zk pour vérifier des attributs (âge, nationalité, qualifications) sans divulguer d'informations personnelles.
- **Jeux et NFTs** : Développement d'états de jeu cachés, d'interactions de joueurs anonymes et de métadonnées NFT secrètes.
- **Vote Privé en Chaîne** : Permet des votes où les votes individuels sont cryptés mais le décompte final est publiquement vérifiable.

Les avantages clés d'Aztec incluent la confidentialité programmable, la réduction significative des coûts de transaction grâce à l'agrégation récursive de preuves, et la sécurité de niveau Ethereum héritée de sa couche de base.

Limites et Perspectives Malgré ses avancées, Aztec Network fait face à des défis tels que la complexité technologique inhérente aux preuves à divulgation nulle de connaissance, la nécessité d'une adoption accrue par les développeurs, et les considérations réglementaires

potentielles liées à la confidentialité. La transition des projets précédents comme Aztec Connect et zk.money vers le L2 complet montre l'évolution stratégique du projet.

L'architecture d'Aztec représente une approche sophistiquée pour combler le fossé entre la transparence blockchain et les exigences de confidentialité du monde réel, positionnant le réseau comme un acteur clé dans la prochaine génération d'infrastructure blockchain.