ALEO - ALEO

Aleo est une blockchain de première couche (Layer 1) conçue pour offrir une confidentialité native grâce à l'intégration des preuves à connaissance zéro (ZKPs). Ces preuves cryptographiques permettent de valider des transactions ou des calculs sans révéler les données sous-jacentes, garantissant ainsi la confidentialité tout en assurant la véracité des opérations. Contrairement à d'autres solutions qui peuvent offrir des fonctionnalités de confidentialité via des mélangeurs (mixers), Aleo intègre la confidentialité au niveau du protocole, chiffrant les transactions par défaut.

L'infrastructure technologique d'Aleo repose sur plusieurs composants clés : snarkOS, un réseau permissionless et scalable pour les contrats intelligents ZK, et snarkVM, une machine virtuelle pour exécuter les calculs. Le protocole de consensus AleoBFT, inspiré des recherches sur Narwhal et Bullshark, assure la sécurité du réseau, complété par un mécanisme de validation et d'exécution appelé "Proof of Succinct Work" qui récompense les "prouveurs" pour les calculs complexes.

Le token ALEO est le moteur de l'écosystème. Son utilité principale inclut :

- **Frais de réseau** : Les utilisateurs paient en ALEO pour les transactions et l'utilisation des dApps.
- **Récompenses** : Les validateurs (qui sécurisent le réseau via le Proof of Stake) et les prouveurs (qui effectuent les calculs ZK) sont récompensés en ALEO.
- **Staking** : Les détenteurs de tokens peuvent staker leurs ALEO pour contribuer à la sécurité du réseau et gagner des récompenses.
- **Gouvernance** : Bien que moins explicitement détaillé, le staking et la possession de tokens sont généralement liés à la gouvernance dans les écosystèmes blockchain.

Aleo se distingue par son potentiel pour une large gamme de cas d'usage, notamment :

- **Finance Décentralisée (DeFi)** : Création d'applications DeFi privées et conformes, comme des systèmes de paiement confidentiels (par exemple, via des partenariats avec Request Finance) ou des stablecoins privés (comme USAD développé avec Paxos Labs).
- **Gestion d'Identité** : Le framework zPass permet la vérification d'identité décentralisée

et l'utilisation de credentials vérifiables tout en protégeant les données personnelles.

- **Santé** : Stockage et partage sécurisés des dossiers médicaux, permettant une divulgation contrôlée aux parties autorisées.
- **Machine Learning** : Développement de modèles de Machine Learning où la confidentialité des données est primordiale.
- **Jeux Vidéo** : Création d'expériences de jeu privées.
- **Vote et Gouvernance** : Systèmes de vote confidentiels pour les organisations décentralisées (DAOs).

Aleo a également développé Leo, un langage de programmation conçu pour simplifier la création d'applications ZK, rendant la technologie plus accessible aux développeurs. Le projet a levé des fonds significatifs auprès d'investisseurs de renom, soulignant la confiance dans son approche axée sur la confidentialité. Malgré ses avantages en matière de confidentialité et de scalabilité, des défis tels que la courbe d'apprentissage potentielle et la taille encore limitée de l'écosystème peuvent être considérés comme des limites actuelles. Les perspectives d'Aleo résident dans sa capacité à devenir une infrastructure fondamentale pour un web plus privé et sécurisé.