ZAMA - Zama

Zama est un projet ambitieux qui vise à résoudre le problème de la transparence intrinsèque des blockchains publiques en intégrant le chiffrement entièrement homomorphe (FHE). Le FHE est une technologie cryptographique avancée qui permet d'effectuer des calculs sur des données chiffrées sans jamais avoir à les déchiffrer. Cela signifie que des informations sensibles, comme les soldes de comptes, les montants de transaction ou l'état d'un contrat intelligent, peuvent être traitées sur la blockchain tout en restant privées.

Le protocole Zama n'est pas une nouvelle blockchain indépendante, mais plutôt une couche d'infrastructure qui peut être intégrée aux blockchains existantes (Ethereum, Solana, etc.) et à leurs solutions de mise à l'échelle (Layer 2). Il est souvent comparé à la "couche HTTPS" pour la blockchain, car il apporte une sécurité et une confidentialité similaires à celles de l'internet sécurisé aux applications décentralisées (dApps).

Le fonctionnement repose sur l'utilisation de coprocesseurs pour décharger les calculs FHE intensifs de la chaîne principale. Cela permet de maintenir des frais de transaction bas tout en assurant la scalabilité et la vérifiabilité publique des opérations. Les développeurs peuvent ainsi créer des contrats intelligents confidentiels, des applications de finance décentralisée (DeFi) privée, des systèmes de vote privés, ou encore gérer des identités numériques de manière sécurisée.

Le token ZAMA joue un rôle central dans l'écosystème Zama. Il est utilisé comme :

- **Token d'utilité :** Pour payer les frais de services du protocole, tels que le chiffrement, le déchiffrement et le pontage de données. Ces frais sont généralement brûlés, créant un mécanisme déflationniste.
- **Staking et sécurité :** Les détenteurs de ZAMA peuvent staker leurs tokens pour sécuriser le réseau, soit en devenant opérateurs (coprocesseurs, nœuds de gestion de clés), soit en déléguant leurs tokens à ces opérateurs. Cela s'inscrit dans un modèle de type "Delegated Proof-of-Stake".
- **Gouvernance :** Les détenteurs de ZAMA peuvent participer aux décisions concernant l'évolution du protocole.

Les récompenses pour les opérateurs et les stakers sont générées par une inflation

contrôlée (minting). Le protocole utilise un modèle "burn-and-mint" pour équilibrer l'offre et la demande du token.

Zama a levé des fonds significatifs auprès d'investisseurs de premier plan, soulignant la confiance dans sa technologie et son potentiel de marché. L'entreprise met l'accent sur l'open-source et vise à rendre le FHE accessible aux développeurs sans nécessiter une expertise cryptographique approfondie, notamment à travers des outils comme fhEVM (pour les blockchains compatibles EVM) et Concrete ML (pour l'IA).

En résumé, Zama apporte une solution innovante à l'un des défis majeurs de la blockchain : la confidentialité. En rendant le traitement des données chiffrées pratique et évolutif, Zama ouvre la porte à une nouvelle génération d'applications blockchain plus sécurisées et conformes aux réglementations, particulièrement dans les secteurs sensibles comme la finance et les données d'entreprise.