ZAMA - Zama

Zama est un projet de cryptographie open-source dont l'ambition est de rendre le chiffrement entièrement homomorphe (FHE) accessible aux développeurs pour l'intégrer aux blockchains. Le protocole Zama fonctionne comme une couche de confidentialité qui peut être superposée à des blockchains existantes (Layer 1 ou Layer 2) telles qu'Ethereum ou Solana, sans nécessiter de modification de leur infrastructure. L'innovation majeure réside dans sa capacité à permettre aux contrats intelligents d'effectuer des calculs sur des données chiffrées, sans jamais avoir à les déchiffrer au préalable. Ce mécanisme assure une confidentialité de bout en bout pour les applications décentralisées.

La technologie FHE est au cœur du fonctionnement de Zama. Elle permet d'effectuer des opérations mathématiques directement sur des données chiffrées, produisant un résultat chiffré qui ne peut être déchiffré que par le détenteur de la clé appropriée. Pour gérer la complexité computationnelle du FHE, Zama utilise un modèle de coprocesseurs qui décharge le travail de la chaîne principale, dans le but de maintenir des frais de transaction bas et de supporter la scalabilité. Le protocole intègre des outils pour les développeurs, notamment des types de données chiffrées spécifiques (comme `euint`) pour marquer les éléments privés dans les contrats intelligents compatibles Solidity.

Le token ZAMA est l'actif utilitaire natif de l'écosystème Zama. Il remplit plusieurs fonctions clés :

- **Frais de protocole :** Les utilisateurs paient en ZAMA pour exécuter des transactions confidentielles et des contrats intelligents. Ces frais sont ensuite brûlés, créant une pression déflationniste.
- **Staking et sécurité du réseau :** Les détenteurs de ZAMA peuvent staker leurs tokens pour sécuriser le réseau, notamment en opérant des nœuds FHE ou des nœuds KMS (Key Management Service). En retour, ils reçoivent des récompenses sous forme de nouveaux tokens (inflation), dans un modèle de "burn-and-mint".
- **Gouvernance :** Les détenteurs de tokens peuvent participer aux décisions concernant les mises à jour du protocole et les changements de paramètres.
- **Incitations pour les opérateurs :** Les opérateurs réseau qui effectuent les calculs FHE intensifs (preuve et vérification) sont récompensés en ZAMA.

Le tokenomics de ZAMA est basé sur un modèle "burn-and-mint". 100% des frais de protocole sont brûlés, tandis que de nouveaux tokens sont frappés pour récompenser les opérateurs et les stakers. L'offre totale de ZAMA est plafonnée à 11 milliards de tokens. Une allocation est prévue pour l'équipe, les investisseurs (VC, anges), la trésorerie, la vente publique et le développement de l'écosystème.

Les cas d'usage potentiels de la technologie Zama sont vastes et ouvrent de nouvelles perspectives pour les applications blockchain nécessitant une protection des données :

- **DeFi Confidentielle :** Permet des échanges, prêts et emprunts sans révéler les positions ou stratégies, prévenant ainsi le front-running.
- **Identité On-chain :** Possibilité de prouver certains attributs (ex: avoir plus de 18 ans) sans révéler l'identité complète ou des documents sensibles.
- **Vote Chiffré (DAOs) :** Permet des votes secrets dans les organisations autonomes décentralisées pour prévenir la coercition.
- **Tokenisation d'actifs réels (RWA) :** Gestion et échange d'actifs tout en préservant la confidentialité des transactions.
- **Paiements Chiffrés :** Transactions où les montants et les détails restent privés.

Zama se positionne comme la "couche HTTPS" pour la blockchain, apportant une fonctionnalité de confidentialité manquante aux réseaux existants. Ses avantages incluent la préservation de la composabilité et de la décentralisation, sans nécessiter d'hypothèses supplémentaires au-delà de la sécurité cryptographique. Cela rend Zama attractif pour des secteurs tels que la finance institutionnelle, la gestion d'identité, les données de santé et l'adoption par les entreprises. Cependant, la complexité du FHE et la nécessité de coprocesseurs dédiés peuvent présenter des défis en termes de performance et de scalabilité à très grande échelle, bien que Zama travaille à optimiser ces aspects avec des améliorations de vitesse et l'anticipation d'accélérateurs matériels FHE dédiés.