NIL - Nillion

Nillion est un réseau informatique décentralisé qui se positionne comme le premier "ordinateur aveugle" au monde, offrant des capacités de calcul et de stockage de données hautement sécurisées et privées. Son objectif principal est de résoudre le problème de la confidentialité des données dans le traitement des informations de grande valeur, un défi majeur pour les blockchains et les réseaux d'IA actuels.

La technologie fondamentale de Nillion repose sur le concept de "calcul aveugle" (blind computation). Ce processus permet d'effectuer des calculs sur des données cryptées sans jamais avoir besoin de les déchiffrer. Cela est rendu possible par l'intégration de diverses technologies d'amélioration de la confidentialité (PETs), telles que le calcul multipartite sécurisé (MPC), le chiffrement entièrement homomorphe (FHE) et les preuves à divulgation nulle de connaissance (ZKP). Nillion combine ces technologies pour créer une couche fondamentale de cryptographie et de calcul aveugle.

Le réseau Nillion est architecturé en couches pour gérer efficacement ses opérations. Il comprend une couche de coordination (Coordination Layer), qui agit comme l'épine dorsale transactionnelle du réseau, gérant les paiements, l'allocation des ressources et les requêtes entre les participants. Cette couche est souvent construite sur des technologies similaires à celles des blockchains et peut être accessible via des wallets comme Keplr et Leap. La couche d'orchestration (Orchestration Layer) est responsable du traitement des données et utilise les PETs pour effectuer les calculs aveugles. Le réseau est composé de nœuds spécialisés : les nœuds nilCC pour le calcul privé, les nœuds nilDB pour le stockage de données cryptées et distribuées, et les nœuds nilAI pour l'exécution d'inférences IA privées.

Le token NIL est le jeton utilitaire natif du réseau Nillion. Il remplit plusieurs fonctions essentielles : il est utilisé pour sécuriser le réseau par le biais du staking (mécanisme de Preuve d'Enjeu Déléguée), où les détenteurs de tokens gagnent du pouvoir de vote pour sécuriser le réseau et décider qui fait partie de l'ensemble actif des validateurs. Les utilisateurs doivent payer des tokens NIL pour accéder aux ressources réseau, effectuer des transactions sur la couche de coordination et lancer des requêtes de calcul aveugle, ce qui permet de gérer efficacement les ressources du réseau. Les fournisseurs d'infrastructure qui participent à des clusters pour faciliter le calcul aveugle et le stockage sécurisé sont

récompensés en NIL. De plus, les détenteurs de tokens NIL participent à la gouvernance décentralisée, proposant et votant sur des décisions critiques concernant le protocole, les paramètres du réseau et les initiatives communautaires.

Les cas d'usage potentiels de Nillion sont vastes et incluent l'IA personnalisée, où les modèles d'IA peuvent être entraînés et utilisés sur des données privées ; les bases de données cryptées ; les marchés de données sécurisés ; les applications financières décentralisées (DeFi) avec des carnets d'ordres entièrement privés ; et les applications de santé où la collaboration sur des données sensibles est nécessaire tout en maintenant une confidentialité stricte. Plus de 35 entreprises ont déjà noué des partenariats avec Nillion pour construire sur son réseau, couvrant des domaines variés tels que l'IA, la DeFi, la gestion des clés, les wallets, l'identité et la messagerie.

Concernant la tokenomics, l'offre totale de NIL est fixée à 1 000 000 000 tokens. Le projet travaille également à affiner sa tokenomics pour assurer la durabilité et la croissance de l'écosystème, en explorant divers mécanismes de combustion (burn) et structures d'incitation. Nillion vise à faire du token NIL un élément essentiel de toutes les opérations du réseau.

En résumé, Nillion représente une avancée significative dans le domaine du traitement des données privées. En offrant une solution de calcul aveugle sécurisée et décentralisée, il ouvre la voie à de nouvelles applications et paradigmes, tout en renforçant la confidentialité et la sécurité des données à l'ère numérique.