

FOLD - The Interfold

The Interfold est un réseau décentralisé axé sur la coordination confidentielle, permettant à des parties indépendantes de générer des résultats partagés et vérifiables à partir d'entrées privées, sans avoir besoin de garde tierce, d'exposition de données ou de dépendance à du matériel de confiance. Il vise à résoudre le problème de la confidentialité dans les blockchains publiques où les transactions sont transparentes, ce qui est problématique pour les cas d'usage nécessitant la discrétion de données sensibles.

Fonctionnement et Technologie : Le réseau repose sur une combinaison d'outils cryptographiques, notamment le chiffrement entièrement homomorphe, les preuves à divulgation nulle de connaissance (zero-knowledge proofs) et le déchiffrement par seuil. Les données entrent dans le système déjà chiffrées. Des opérateurs indépendants, appelés ciphernodes, traitent ces données chiffrées directement, sans jamais les déchiffrer. Une fois que le groupe valide le résultat, seule la réponse finale est publiée. Les entrées brutes ne sont jamais révélées, et aucun opérateur individuel ne contrôle le processus de manière unilatérale. Cette architecture garantit que les entrées privées peuvent mener à des résultats partagés sans que les données sous-jacentes ne soient exposées ni qu'un seul acteur ne contrôle l'exécution, la vérification ou la libération des résultats.

Utilité du Token FOLD : Le token FOLD est le pilier économique et opérationnel de The Interfold. Son utilité est multiple :

- Participation et Coordination : Les opérateurs de ciphernodes doivent staker (mettre en jeu) des tokens FOLD pour participer aux responsabilités du réseau, assurant ainsi la sécurité des processus cryptographiques décentralisés sous-jacents aux Environnements d'Exécution Chiffrés (E3).
- Incitations Économiques : FOLD est utilisé pour récompenser les opérateurs pour leur contribution au réseau et pour gérer l'économie des requêtes au sein des E3.
- Gouvernance : Le token donne le droit de participer à la gouvernance du réseau, permettant aux détenteurs de prendre des décisions concernant son évolution.
- Cautionnement des Opérateurs : FOLD est utilisé pour le cautionnement des opérateurs, créant une responsabilité économique pour garantir leur bon comportement.

Tokenomics : Le FOLD dispose d'une offre maximale fixe de 1,2 milliard de tokens, sans possibilité de création de nouveaux tokens (pas de fonction de mint). Au moment de l'événement de génération de tokens (TGE), l'offre en circulation devrait être de 30 % ou moins, le reste étant bloqué et débloqué progressivement. La répartition de l'offre est la suivante : environ 54,5 % sont destinés aux initiatives orientées communauté (Trésorerie, CCA, Airdrops), tandis que les 45,5 % restants couvrent Gnosis Guild, les investisseurs et l'équipe principale. Cette structure vise à assurer une distribution équilibrée et à aligner les incitations à long terme.

Cas d'Usage : Le réseau Interfold, à travers son implémentation Network Alpha, est conçu pour des cas d'usage concrets nécessitant confidentialité et vérifiabilité :

- **Gouvernance Confidentielle :** Intégré avec Aragon, il permet des votes chiffrés où les résultats sont vérifiables sans révéler l'intention de vote individuelle, réduisant ainsi les risques de coercition ou d'achat de votes.
- **Enchères Scellées :** Permet de soumettre des offres confidentielles qui sont ensuite traitées pour déterminer le gagnant sans que les offres individuelles soient connues avant la clôture.
- **Sondages Secrets :** Permet de réaliser des sondages où les réponses individuelles restent privées.
- **Analyse Collaborative de Données :** Les entreprises peuvent analyser des ensembles de données partagés sans révéler leurs données brutes respectives.
- **Coordination Multi-Agents :** Facilite la coordination entre différents agents ou systèmes nécessitant des informations privées pour parvenir à un résultat commun.

Perspectives : The Interfold se positionne comme une infrastructure essentielle pour la « coordination confidentielle », un domaine de plus en plus critique dans l'écosystème Web3. En fournissant les outils pour des calculs privés et vérifiables, il ouvre la voie à une nouvelle génération d'applications décentralisées où la confidentialité n'est plus un obstacle. Le projet, anciennement connu sous le nom d'Enclave, vise à être le fondement technologique pour des solutions de confidentialité avancées, plutôt qu'une application spécifique.