HOPR - HOPR

Le protocole HOPR (prononcé 'hopper') est une solution de confidentialité axée sur la communication décentralisée et sécurisée. Son objectif principal est de permettre aux individus et aux entreprises d'échanger des informations en ligne de manière totalement privée, en garantissant qu'aucun tiers ne puisse connaître les données partagées, leur volume, ni les expéditeurs ou destinataires.

Fonctionnement et Technologie : HOPR fonctionne grâce à un réseau incitatif de pairs à pairs (mixnet) où les messages sont relayés à travers plusieurs "sauts" (hops) par des nœuds uniques. Cette architecture utilise la technologie "Sphinx packet", qui formate les paquets de données de manière à ce qu'ils apparaissent tous identiques, rendant difficile la fuite d'informations sur l'expéditeur, le destinataire ou le contenu du message.

Le réseau est sécurisé par un mécanisme appelé "proof-of-relay". Ce système cryptographique récompense les opérateurs de nœuds avec des tokens HOPR uniquement après qu'ils aient correctement relayé les données. Cela garantit un comportement honnête et incite à la participation au réseau. Les nœuds peuvent être exécutés sur divers appareils, y compris des ordinateurs personnels ou des appareils connectés à un routeur, éliminant le besoin de serveurs centralisés. HOPR se positionne comme un protocole de couche 0 (Layer 0), intégrant la confidentialité dès la fondation de son architecture.

Le Token HOPR : Utilité et Tokenomics : Le token HOPR est un token utilitaire ERC-20 sur la blockchain Ethereum. Il remplit trois fonctions principales au sein de l'écosystème :

1. **Payer (Pay) :** Les utilisateurs dépensent des tokens HOPR pour envoyer des données privées à travers le réseau. Chaque relais perçoit une partie du paiement.
2. **Staker (Stake) :** Les opérateurs de nœuds bloquent des tokens HOPR pour pouvoir relayer davantage de données et gagner des récompenses sous forme de tokens HOPR. Ces récompenses proviennent à la fois du trafic utilisateur et du "cover traffic" (trafic de camouflage) qui assure l'anonymat même en cas de faible utilisation du réseau.
3. **Voter (Vote) :** Les détenteurs de tokens HOPR participent à la gouvernance décentralisée du protocole (DAO), pouvant voter sur les paramètres du protocole et

d'autres propositions.

La supply totale de tokens HOPR est de 1 milliard. La distribution initiale a alloué environ 25,5% à la trésorerie, 25% au trafic de couverture, 18,5% à l'équipe et aux conseillers, 16,5% aux premiers acheteurs de tokens et le reste à d'autres usages.

Cas d'Usage et Avantages : HOPR offre une confidentialité complète pour les données et les messages, ce qui est essentiel dans un monde où les métadonnées sont de plus en plus exploitées. Des applications comme RPCh (RPC over HOPR) sont déjà développées pour apporter plus de confidentialité aux portefeuilles crypto et aux applications de finance décentralisée (DeFi) en masquant les métadonnées associées aux appels RPC. Le protocole vise à devenir une infrastructure de base pour la confidentialité dans le Web3, permettant aux développeurs de créer des applications véritablement privées. Sa nature incitative et sa scalabilité le distinguent des technologies de mixnet plus anciennes.

Gouvernance et Organisation : Le contrôle et la gestion de l'infrastructure du réseau sont décentralisés et confiés aux utilisateurs via le token HOPR et une DAO. L'Association HOPR, une entité à but non lucratif basée en Suisse, assure la couverture légale du projet lorsqu'il interagit dans le monde réel, protégeant ainsi l'identité de ses détenteurs.

Développement et Perspectives : HOPR a obtenu un brevet américain pour sa technologie de communication sécurisée, étendant ses capacités à des environnements cloud. Le projet collabore activement avec d'autres projets du Web3 pour intégrer des solutions de confidentialité à divers niveaux de l'écosystème. Les perspectives incluent l'expansion de son réseau, le développement de nouvelles applications privées et l'amélioration continue de son protocole pour répondre aux défis croissants de la vie privée numérique.