GPS - GoPlus Security

GoPlus Security (GPS) se positionne comme la première couche de sécurité décentralisée pour le Web3, conçue pour offrir une protection complète à travers tous les réseaux blockchain. Son objectif principal est de créer un environnement d'interaction on-chain plus sûr et plus convivial en comblant les lacunes de sécurité inhérentes à l'architecture blockchain actuelle.

Fonctionnement et Technologie : Le protocole repose sur une architecture modulaire qui combine plusieurs éléments clés :

- **Couche de Données de Sécurité :** Elle agrège et valide les données de menace provenant de divers contributeurs, y compris les utilisateurs, les chercheurs et les entreprises de sécurité. Cette approche décentralisée garantit l'intégrité et la fiabilité des données collectées.
- **Couche de Calcul :** En tirant parti des Services Validés Activement (AVS) d'Eigenlayer, cette couche effectue des analyses de risques décentralisées. Des nœuds distribués, appelés Opérateurs AVS, réalisent des calculs et des validations de sécurité, évaluant les transactions pour détecter les menaces potentielles et assurant ainsi la scalabilité et la résilience du réseau.
- **Protocole SecWare :** Il permet aux développeurs de créer et de proposer des modules de sécurité personnalisés, tels que SafeToken pour le lancement sécurisé de tokens et la gestion de liquidité. Cela favorise un écosystème ouvert et collaboratif pour le développement de solutions de sécurité.
- **Intelligence Artificielle (IA) :** GoPlus intègre l'IA pour des audits de contrats intelligents avancés, la prédiction de menaces, la simulation de transactions afin d'évaluer les risques potentiels avant leur exécution, la détection d'adresses malveillantes et l'analyse des risques des contrats intelligents. Ces outils automatisés aident les utilisateurs à éviter les arnaques et les transactions risquées.

GoPlus prend en charge plus de 30 chaînes, y compris Ethereum, Solana et BNB Chain, et a protégé des millions de portefeuilles, détectant des centaines de milliers d'actifs malveillants.

Utilité et Cas d'Usage du Token GPS : Le token GPS est au cœur de l'écosystème GoPlus Security et possède plusieurs utilités principales :

- **Paiement pour les Services de Sécurité :** Les utilisateurs et les entreprises paient en GPS pour accéder aux divers services de sécurité offerts par GoPlus, tels que les analyses de risque, l'accès aux API et les fonctionnalités premium.
- **Staking :** Les contributeurs, tels que les fournisseurs de données et les opérateurs de nœuds de calcul, doivent staker des tokens GPS pour participer au réseau. En retour, ils sont récompensés pour leurs contributions et pour l'aide apportée à la sécurisation du réseau.
- **Gouvernance :** Les détenteurs de tokens GPS peuvent participer à la gouvernance du réseau. En stakant leurs tokens, ils acquièrent un poids de vote pour proposer et approuver des mises à jour du protocole, des modifications des paramètres de sécurité et d'autres décisions importantes pour l'écosystème. Ce mécanisme de gouvernance basé sur le staking encourage un engagement à long terme et une participation responsable.
- **Réduction des Frais :** Les détenteurs de GPS peuvent bénéficier de réductions sur les frais de transaction et les services de sécurité.

Tokenomics : L'offre totale de tokens GPS est de 10 milliards. L'allocation est la suivante : environ 24,67 % pour la communauté et le développement, 20 % pour l'équipe (avec une période de vesting), et 19,33 % pour les premiers investisseurs. Les revenus de GoPlus proviennent des abonnements SaaS et des frais de transaction. Une partie des revenus est utilisée pour le rachat et le brûlage de tokens GPS, créant ainsi un modèle déflationniste.

Avantages et Limites : GoPlus Security offre une approche complète et décentralisée de la sécurité Web3, intégrant l'IA et des technologies avancées pour une protection en temps réel. Sa capacité à s'intégrer à diverses blockchains et projets le rend particulièrement pertinent. Cependant, comme pour tout projet décentralisé, des défis subsistent concernant la complexité de la gouvernance, la nécessité d'une adoption généralisée pour maximiser son efficacité, et la nécessité de maintenir une transparence totale sur les protocoles de stockage et d'accès aux données pour garantir la confiance.

Perspectives : Avec la croissance continue de l'écosystème Web3 et l'augmentation des menaces de sécurité, des solutions comme GoPlus Security sont de plus en plus essentielles. Le projet vise à établir des normes de sécurité plus élevées dans l'espace

Web3, en devenant une infrastructure fondamentale pour la protection des utilisateurs et des actifs numériques. Les développements futurs incluent l'expansion des intégrations de chaînes, le lancement d'un portail de gouvernance et l'intégration de services de sécurité tiers.