PROVE - Succinct

Succinct est un protocole centré sur le calcul vérifiable qui permet aux développeurs de générer et de vérifier facilement des preuves à connaissance nulle (ZKP) dans divers contextes grâce à sa machine virtuelle ZK (zkVM) à usage général. L'objectif de Succinct est de faire de la vérifiabilité cryptographique une fonctionnalité par défaut dans l'infrastructure blockchain et web3, la rendant plus scalable, sécurisée et minimisant la confiance. Le projet est conçu pour simplifier l'intégration des ZKP en permettant aux développeurs d'écrire des programmes vérifiables dans des langages familiers comme Rust, réduisant ainsi le temps d'intégration de mois à quelques jours. La technologie de Succinct trouve des applications réelles dans le support des solutions de rollup de couche 2, des échanges vérifiables, des ponts inter-chaînes sans confiance, la vérification des calculs hors chaîne, et même la vérification de modèles d'IA et les systèmes de préservation de la vie privée.

Le réseau Succinct Prover fonctionne comme un marché décentralisé sur Ethereum. Les applications soumettent des demandes de génération de preuves à connaissance nulle, et des provers indépendants entrent en concurrence pour les vérifier et les produire en échange de récompenses. Ce système utilise un mécanisme d'enchères hors chaîne pour faire correspondre les demandes aux provers, avec des résultats réglés sur la chaîne via des contrats intelligents. Le réseau est conçu pour ressembler à une application web rapide et réactive, tout en garantissant une sécurité cryptographique et une vérifiabilité sur la chaîne.

Le token PROVE est le jeton utilitaire natif de l'écosystème Succinct. Il s'agit d'un token ERC-20 émis sur Ethereum. Sa fourniture totale est fixe à 1 000 000 000 de tokens PROVE. Les principaux cas d'usage du token PROVE incluent :

- **Paiement :** Les utilisateurs (comme les rollups, les ponts ou les dApps) paient les provers en PROVE pour la génération de preuves.
- **Staking :** Les provers peuvent staker des tokens PROVE pour participer aux enchères et obtenir des tâches. Un staking plus important peut permettre de traiter plus de requêtes. Cependant, le non-respect des délais ou la soumission de preuves erronées peuvent entraîner la confiscation (slashing) d'une partie de leur mise.
- **Gouvernance :** Les détenteurs de PROVE peuvent participer à la gouvernance du

réseau, en votant sur les paramètres du protocole tels que les émissions, la conception des enchères et les structures de frais.

Le réseau Succinct Prover vise à démocratiser l'accès à l'infrastructure ZKP, la rendant plus rapide, moins chère et plus facile à utiliser pour les développeurs. Cela élimine le besoin de configurations personnalisées et de connaissances cryptographiques approfondies, facilitant ainsi l'intégration de technologies ZKP dans une large gamme d'applications décentralisées. Le projet a été fondé par Uma Roy et John Guibas et a reçu le soutien d'investisseurs de premier plan tels que Paradigm. L'approvisionnement total du token PROVE est de 1 000 000 000 de tokens, avec une distribution prévue pour le développement du réseau, la participation communautaire et la croissance de l'écosystème.