PEARL - Pearl

Pearl est une blockchain de couche 1, lancée le 27 avril 2026, qui dérive de Bitcoin mais propose une approche révolutionnaire pour le mécanisme de consensus. Elle remplace le processus de hachage SHA-256 de Bitcoin, qui consomme beaucoup d'énergie et dont le calcul n'a pas d'utilité extérieure, par un système appelé "Proof of Useful Work" (PoUW). Ce mécanisme PoUW consiste pour les mineurs à effectuer des multiplications de matrices (MatMul), qui sont au cœur de l'entraînement et de l'inférence des modèles d'intelligence artificielle. L'idée est que les GPUs, utilisés intensivement dans l'IA, puissent simultanément sécuriser le réseau Pearl et effectuer des calculs utiles pour des clients IA. Cela permettrait aux mineurs de générer des revenus à partir des récompenses de bloc et potentiellement de frais pour les calculs IA, rendant le minage plus rentable et durable.

Sur le plan technologique, Pearl conserve le modèle UTXO de Bitcoin et utilise une base de code dérivée de btcd, une implémentation Bitcoin en Go. La différence clé réside dans la fonction de travail : les mineurs soumettent des matrices à multiplier, et le réseau vérifie que la multiplication a eu lieu et qu'elle était suffisamment difficile, sans nécessairement vérifier l'utilité spécifique du résultat. La conception repose sur des recherches académiques qui suggèrent que l'ajout de la preuve de travail à la multiplication de matrices n'entraîne qu'un surcoût négligeable.

Le jeton natif de Pearl est le PRL. Il possède une offre maximale fixe de 2,1 milliards de jetons, ce qui est 100 fois l'offre de Bitcoin. Il n'y a pas de pré-minage ; tous les jetons sont mis en circulation par le biais des récompenses de bloc. La courbe d'émission des récompenses est conçue pour décroître de manière polynomiale, de sorte que près de la moitié de l'offre totale soit minée au cours des quatre premières années, ce qui vise à réduire l'inflation au fil du temps. Les récompenses de minage diminuent légèrement à chaque bloc, sans événements de "halving" traditionnels comme ceux de Bitcoin. La distribution des jetons est donc principalement déterminée par les règles de minage et l'historique du lancement. Il existe une légère divergence dans les chiffres de l'offre en circulation rapportés par différentes sources, qui peut être due à des méthodes de suivi différentes. Le projet a une politique de vesting linéaire pour les récompenses de minage, avec un calendrier complet s'étendant jusqu'en 2051.

L'utilité du jeton PRL se concentre principalement sur les récompenses de minage et les frais de transaction. Il peut également servir de subvention pour les opérateurs qui vendent le PRL gagné en servant des modèles d'IA pour compenser leurs coûts. Le projet a établi un partenariat avec Together AI, qui utilise cette approche pour financer ses services d'inférence à prix réduit, démontrant ainsi le modèle économique. D'autres utilisations incluent des primes de sécurité pour les rapports de bugs.

La gouvernance de Pearl semble minimaliste, s'alignant sur l'éthos de Bitcoin où les changements sont adoptés par consensus communautaire et adoption par les nœuds.

Les avantages potentiels de Pearl incluent la fusion de la sécurité blockchain avec des calculs IA économiquement viables, une approche "fair launch" qui évite le sentiment anti-VC, et des unités économiques combinées où les GPUs peuvent gagner des revenus de l'inférence et du minage. Cependant, des limites existent. Une étude indépendante a relevé que le logiciel de minage mesuré ne produisait pas de sortie IA utile, suggérant que les mineurs pourraient exécuter des calculs aléatoires moins coûteux. Le protocole actuel ne peut pas prouver de manière fiable que les calculs proviennent de clients IA réels et payants. L'équipe reconnaît ce problème et prévoit des mises à jour pour rendre le minage "pur" plus coûteux que l'inférence réalisée "en sous-produit".

En résumé, Pearl est une expérience ambitieuse visant à transformer le PoW en un système plus axé sur l'utilité, alignant les incitations du minage avec la demande croissante de puissance de calcul pour l'IA. Son succès dépendra de sa capacité à garantir que le travail effectué par les mineurs soit véritablement utile pour l'IA et que le protocole puisse évoluer pour le prouver de manière plus robuste.