QRL - Quantum Resistant Ledger

Le Quantum Resistant Ledger (QRL) est une plateforme blockchain pionnière, développée dans le but de contrer les menaces potentielles posées par l'avènement des ordinateurs quantiques. L'architecture fondamentale de QRL est conçue pour offrir une sécurité post-quantique robuste, garantissant la protection des actifs numériques et des communications à long terme. Contrairement à de nombreuses blockchains existantes qui s'appuient sur la cryptographie à courbe elliptique (ECC) ou l'ECDSA, potentiellement vulnérables aux futures capacités de calcul quantique, QRL intègre nativement le schéma de signature eXtended Merkle Signature Scheme (XMSS).

XMSS est une méthode cryptographique basée sur des fonctions de hachage, reconnue pour sa résistance aux attaques quantiques, et elle est spécifiée par l'IETF et approuvée par le NIST. Cette technologie cryptographique garantit que les signatures numériques créées sur le réseau QRL restent sécurisées, même face aux avancées de l'informatique quantique. QRL a été lancé en juin 2018 et fonctionne initialement sur un consensus Proof-of-Work (PoW) utilisant l'algorithme RandomX, favorisant le minage par CPU. Le projet est en cours de transition vers un mécanisme de consensus Proof-of-Stake (PoS) avec l'objectif d'améliorer l'efficacité énergétique et la scalabilité.

Les cas d'usage et fonctionnalités de QRL incluent :

- **Sécurité Post-Quantique des Actifs Numériques :** QRL offre un stockage de valeur sécurisé et pérenne, protégeant les cryptomonnaies contre les futures vulnérabilités quantiques.
- **Communications Sécurisées :** Le réseau propose une couche de communication décentralisée offrant une messagerie chiffrée et sécurisée, résistant aux menaces quantiques.
- **Messagerie sur Chaîne :** Permet l'envoi de messages courts (jusqu'à 80 octets) directement sur la blockchain.
- **Notarisation de Documents :** La plateforme permet la notarisation de documents de

manière post-quantique, assurant leur intégrité et leur authenticité.

- **Adresses Réutilisables :** Pour une meilleure expérience utilisateur, QRL propose des adresses qui peuvent être utilisées pour plusieurs transactions.
- **Support de Tokens QRT :** La blockchain supporte la création de tokens Quantum Resistant Token (QRT).
- **Compatibilité EVM et Développement d'Applications :** Via son projet "Zond" (QRL 2.0), QRL vise à devenir compatible avec l'Ethereum Virtual Machine (EVM). Cela permettra aux développeurs de déployer des contrats intelligents (smart contracts) écrits en Solidity et de construire des applications décentralisées (dApps) sur une plateforme sécurisée contre les menaces quantiques. Des outils comme le portefeuille d'extension Chrome Zond et un IDE basé sur RemixIDE sont développés pour faciliter la création d'applications.

Concernant la tokenomics, l'offre maximale de QRL est de 105 000 000 Quanta. L'émission des tokens suit un calendrier de décroissance exponentielle sur environ 200 ans. L'offre initiale publique était de 52 000 000 Quanta, avec une offre initiale réservée de 13 000 000 Quanta pour la distribution par la Fondation QRL et d'autres réserves. Le projet met l'accent sur la transparence et le développement communautaire. Le fondateur de QRL est le Dr Peter Waterland.

Les avantages de QRL résident dans sa sécurité avant-gardiste face à la menace quantique, son approche proactive pour l'avenir de la blockchain, ses fonctionnalités variées et son écosystème en développement actif. Les limites potentielles pourraient inclure la complexité de l'adoption massive d'une technologie de niche axée sur la sécurité future, et les défis liés à la transition technologique. Cependant, QRL se positionne comme une solution essentielle pour les entités préoccupées par la longévité et la sécurité de leurs actifs numériques et de leurs infrastructures dans un monde de plus en plus numérisé et potentiellement confronté à de nouvelles capacités de calcul.