# QRL - Quantum Resistant Ledger

Le Quantum Resistant Ledger (QRL) a été conçu dès le départ pour être résistant aux attaques des ordinateurs quantiques, une menace potentielle pour la sécurité des cryptomonnaies actuelles comme le Bitcoin et l'Ethereum. La vulnérabilité découle de l'utilisation de schémas de chiffrement comme l'ECDSA (Elliptic Curve Digital Signature Algorithm), qui pourraient être compromis par l'algorithme de Shor s'il était exécuté sur un ordinateur quantique suffisamment puissant. QRL utilise le schéma de signature XMSS (eXtended Merkle Signature Scheme), un système de signature basé sur des fonctions de hachage qui est approuvé par le NIST et considéré comme résistant aux attaques quantiques. Le XMSS offre une sécurité à long terme en générant des signatures à usage unique, ce qui rend difficile pour les pirates de déchiffrer des transactions passées ou de falsifier de nouvelles transactions. Ce schéma de signature est également réutilisable, ce qui améliore la commodité pour les utilisateurs.

Le réseau QRL fonctionne sur un mécanisme de consensus de preuve d'enjeu décentralisée (dPoS). Ce mécanisme permet aux détenteurs de QRL de participer à la validation des blocs et de sécuriser le réseau tout en gagnant des récompenses, contribuant ainsi à la décentralisation et à la sécurité. Le projet met également l'accent sur la confidentialité des utilisateurs grâce à des fonctionnalités telles que les adresses furtives (stealth addresses) et les signatures d'anneau (ring signatures), qui rendent plus difficile le traçage des transactions.

En termes de tokenomics, l'offre maximale de QRL est de 105 000 000 de tokens, avec une émission qui suit un schéma de décroissance exponentielle sur environ 200 ans. Il y a une réserve de 8 450 000 QRL pour la Fondation QRL. L'inflation actuelle est de 1,1443%. Le projet a été lancé avec une distribution initiale de 52 000 000 Quanta pour la partie publique et 13 000 000 pour les réserves. Les tokens QRL peuvent être utilisés pour l'arbitrage, le staking pour générer des revenus passifs, ou pour d'autres applications financières.

Au-delà de la sécurité quantique, QRL offre plusieurs fonctionnalités avancées : des jetons

résistants aux quantiques (QRT), une API complète pour les développeurs, des portefeuilles multi-signatures, et des capacités de messagerie éphémère. Le projet se veut également convivial, avec des portefeuilles disponibles sur différentes plateformes (desktop, mobile, web) et le support des portefeuilles matériels comme Ledger Nano S & X. Le code source est open-source et a fait l'objet d'audits par des tiers.

Les cas d'usage potentiels de QRL incluent la sécurisation des actifs numériques, mais aussi potentiellement des services de cybersécurité améliorés, des services de messagerie d'entreprise, des identités post-quantiques sécurisées, et la voix sur IP post-quantique. L'accent est mis sur la création d'un écosystème robuste pour les développeurs afin de construire des applications décentralisées sur une base prouvée comme étant résistante aux quantiques.

Les avantages de QRL résident dans sa sécurité avant-gardiste contre les menaces quantiques, son architecture axée sur l'utilisateur, et son écosystème de développement. Les limites pourraient inclure la complexité de la cryptographie post-quantique pour les utilisateurs moins techniques, et la nécessité d'une adoption généralisée pour réaliser son plein potentiel. Les perspectives du projet sont liées à l'évolution de l'informatique quantique et à sa capacité à rester à la pointe des avancées technologiques pour maintenir sa pertinence et sa sécurité.