

QTC - Quantus

Quantus est une blockchain de premier niveau (Layer 1) dont la caractéristique distinctive est sa conception axée sur la sécurité post-quantique et la confidentialité des transactions. Elle utilise le mécanisme de consensus Proof-of-Work (PoW), avec un temps de bloc cible de 12 secondes et une offre maximale fixe de 21 millions de tokens QTC, à l'instar de Bitcoin.

La résistance aux ordinateurs quantiques est au cœur de l'architecture de Quantus. Le réseau intègre des signatures numériques ML-DSA (Magic Lantern Digital Signature Algorithm), un standard post-quantique développé par le NIST (National Institute of Standards and Technology) américain. Cette technologie vise à rendre les transactions et les signatures de Quantus invulnérables aux attaques potentielles des futurs ordinateurs quantiques, un risque identifié pour les signatures à courbe elliptique actuellement utilisées par de nombreuses blockchains, y compris Bitcoin.

Outre la sécurité quantique, Quantus met l'accent sur la confidentialité. Le réseau emploie des preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs) via son système d'adresses "Wormhole". Cette technologie permet de vérifier la validité des transactions sans révéler d'informations sensibles, tout en contribuant à réduire la surcharge de données sur la chaîne causée par les signatures post-quantiques.

Technologiquement, Quantus est construit sur le framework Substrate, un ensemble d'outils de développement blockchain créé par Parity Technologies, également à l'origine de Polkadot. Ce choix d'architecture permet une certaine flexibilité et modularité au réseau.

En termes de tokenomics, 73% de l'offre totale de QTC (environ 15,3 millions de tokens) sont alloués au minage. Les 27% restants (environ 5,67 millions de tokens) ont été créés lors du lancement (genèse). Cette allocation initiale comprend des parts pour les investisseurs (23%), les fondateurs et l'équipe, ainsi que 4% pour l'entreprise. Des calendriers de vesting sont appliqués à ces tokens pré-minés pour éviter une dilution soudaine du marché. Une petite partie de l'allocation de l'entreprise (1% de l'offre totale) a été mise à disposition pour la liquidité initiale au moment de la genèse.

Le lancement du mainnet de Quantus a eu lieu le 9 septembre 2026. Le projet se positionne

non pas comme une plateforme de contrats intelligents généralistes (à la manière d'Ethereum), mais plutôt comme une blockchain axée sur la fonction de "monnaie électronique pair-à-pair", similaire dans sa philosophie à Bitcoin, Monero ou Zcash.

L'un des défis pour Quantus est d'établir sa liquidité et son adoption. Initialement, l'accès au token QTC était principalement limité au minage sur son propre réseau. Cependant, une intégration notable a été réalisée avec NEAR Intents, une plateforme qui permet l'échange d'actifs entre différentes blockchains. Cette intégration permet aux utilisateurs d'acquérir du QTC en utilisant plus de 180 actifs provenant de plus de 30 chaînes différentes, sans avoir recours à des échanges centralisés. Cela offre au QTC sa première véritable voie d'accès à la liquidité inter-chaînes.

Les avantages potentiels de Quantus résident dans son approche proactive de la sécurité quantique, son accent sur la confidentialité et son offre limitée. Cependant, le projet est encore très jeune. Le mainnet n'est opérationnel que depuis peu, et une grande partie des affirmations techniques et des performances proviennent du projet lui-même. Les risques incluent la volatilité du marché, les risques d'implémentation liés à la complexité de la cryptographie post-quantique et des preuves à divulgation nulle, ainsi que la dépendance à l'égard de l'adoption de technologies de sécurité quantique par l'écosystème crypto dans son ensemble. L'avenir de Quantus dépendra de sa capacité à prouver la robustesse de sa technologie sur le long terme et à attirer une base d'utilisateurs et de développeurs.