# Quantus Network Whitepaper

**Autores:** Christopher Smith | **Última actualización:** 14 de enero de 2026

## Introducción

### La amenaza cuántica

Las blockchains tradicionales se enfrentan a una amenaza existencial con el advenimiento de la computación cuántica. Los fundamentos criptográficos de las blockchains se basan en la dureza del problema del logaritmo discreto (DLP), y los algoritmos cuánticos, especialmente el de Shor, pueden resolver el DLP exponencialmente más rápido que los ordenadores clásicos. Esta vulnerabilidad podría permitir a los adversarios cuánticos derivar claves privadas a partir de claves públicas, lo que les permitiría falsificar transacciones y descifrar datos financieros sensibles.

El resultado es un fallo catastrófico del sistema. Sin actualizaciones proactivas resistentes a la computación cuántica, la economía cripto de billones de dólares corre el riesgo de una devaluación repentina por tales ataques.

> 💡 **TIP**
>
> **Quantus soluciona esto.**

### Propuesta de valor única

Nombrada a partir de la palabra latina para “cuánto”, Quantus Network ofrece una preservación de la riqueza escalable y segura desde el punto de vista cuántico. Quantus no es una plataforma de contratos inteligentes. En su lugar, como un restaurante de alta gama sin menú, Quantus se centra en hacer un pequeño número de cosas mejor que cualquier otra chain.

Específicamente, Quantus utiliza:

- signature post-cuánticas para todas las transacciones
- signature y cifrado post-cuánticos (ML-DSA y ML-KEM) para asegurar las conexiones entre pares

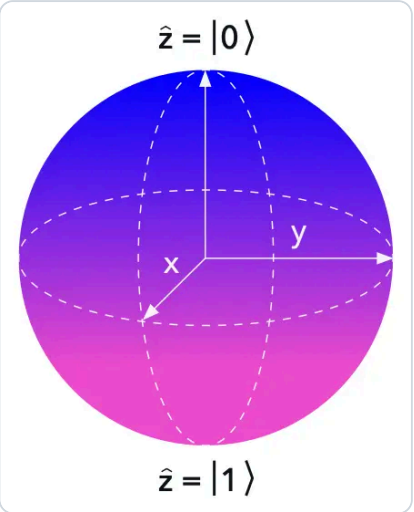
- Un Bridge post-cuántico a otras blockchains y la creación de wrapped coins seguras desde el punto de vista cuántico
- zero-knowledge-proofs post-cuánticas para escalar
- Cuentas de alta seguridad para disuadir el robo y permitir la recuperación tras errores
- check-phrases legibles por humanos para una fácil verificación de direcciones

Este enfoque específico permite a los usuarios preservar su riqueza con confianza, convirtiendo las amenazas cuánticas en oportunidades.

> 💡 **TIP**
> Quantus es la fortaleza a prueba de futuro para su fortuna.

# La amenaza cuántica para la Blockchain

## Conceptos básicos de computación cuántica




Los ordenadores cuánticos aprovechan principios como la superposición y el entrelazamiento para realizar cálculos que son inabordables para las máquinas clásicas.

A diferencia de los bits clásicos, que son 0 o 1, los bits cuánticos (qubits) pueden existir en múltiples estados simultáneamente, lo que permite un paralelismo exponencial para ciertos problemas. **Esta capacidad plantea riesgos existenciales para los sistemas criptográficos que sustentan las finanzas en blockchain, ya que los algoritmos desarrollados para el hardware cuántico socavan los supuestos de seguridad de la mayoría de la criptografía de clave pública.**

### Algoritmo de Shor

Introducido en 1994 por Peter Shor, proporciona un método de tiempo polinómico para factorizar enteros grandes y resolver el problema del logaritmo discreto en un ordenador cuántico. En esencia, explota las Transformadas Cuánticas de Fourier (QFT) para encontrar el periodo de una función, permitiendo la reversión eficiente de las funciones de trampa que subyacen a esquemas como RSA o la criptografía de curva elíptica (ECC).

**Para las finanzas en blockchain, esto significa que un atacante con un ordenador cuántico suficientemente potente (estimado en ~2.300 qubits lógicos) podría derivar claves privadas a partir de claves públicas en tiempo polinómico $O(n^3)$. Esto supone una aceleración extrema, dejando obsoletos los sistemas vulnerables de la noche a la mañana.**

### Algoritmo de Grover

Propuesto por Lov Grover en 1996, ofrece una aceleración cuadrática para problemas de búsqueda no estructurados, reduciendo el tiempo para encontrar un elemento específico en una base de datos desordenada de $O(n)$ a $O(\sqrt{n})$ operaciones. Funciona amplificando iterativamente la amplitud del estado objetivo mediante interferencia

cuántica. Aunque no es tan devastador como el de Shor para la criptografía asimétrica, **el de Grover impacta en primitivas simétricas como las funciones hash y el cifrado AES, reduciendo efectivamente a la mitad el nivel de seguridad** (por ejemplo, una clave de 256 bits se comporta como una de 128 bits frente a ataques cuánticos).

Aunque impactante, este ataque se mitiga simplemente duplicando los bits de seguridad, en lugar de cambiar el esquema criptográfico. Además, la aceleración cuadrática de Grover es poco práctica debido a sus altos requisitos de qubits y puertas, requiriendo miles de millones de operaciones en secuencia, con una paralelización limitada, lo que la hace inviable para reversiones en el mundo real incluso en hardware futuro.

## Los peligros de la computación cuántica para las finanzas en blockchain pueden categorizarse en cuatro áreas:

### Falsificación de signature digitales

El algoritmo de Shor amenaza directamente las signature basadas en ECC utilizadas en la mayoría de las blockchains (por ejemplo, la curva secp256k1 de Bitcoin), lo que permite a los adversarios suplantar a los usuarios y autorizar transacciones fraudulentas. Tal capacidad representaría un fallo crítico de la característica más básica de una blockchain.

### Falsificación de pruebas falsas en sistemas de conocimiento cero

Muchos zero-knowledge proofs, como los de zk-SNARKs para finanzas centradas en la privacidad, se basan en la dureza del logaritmo discreto a través de emparejamientos de curvas elípticas para los compromisos; el de Shor podría permitir la creación de pruebas inválidas que parezcan válidas, lo que podría permitir a un atacante acuñar nuevas monedas o falsificar el estado de las Capas 2 (L2).

### Descifrado de información secreta

Los ataques cuánticos podrían exponer datos cifrados protegidos por esquemas de clave pública vulnerables en protocolos de privacidad como Zcash o Monero. También podrían descifrar las comunicaciones p2p en protocolos financieros, revelando detalles sensibles de la riqueza y permitiendo robos selectivos.

### Reversión de funciones hash

El algoritmo de Grover podría acelerar los ataques de preimagen en hashes como SHA-256, utilizados para el proof-of-work y la generación de direcciones, pero esta es la amenaza menos preocupante. Muchos esquemas criptográficos post-cuánticos

incorporan construcciones basadas en hash, ya que los hashes se consideran lo suficientemente seguros con un resumen lo suficientemente grande.

## Desafíos de escalado en la criptografía post-cuántica

Si bien la criptografía post-cuántica (PQC) ofrece protecciones esenciales contra las amenazas cuánticas, introduce importantes obstáculos de escalado debido al diseño inherente de estos algoritmos. A diferencia de los esquemas de curva elíptica, que se basan en estructuras matemáticas compactas, las primitivas PQC requieren parámetros más grandes para mantener la seguridad contra adversarios tanto clásicos como cuánticos. Esto da como resultado claves públicas, claves privadas y signature sustancialmente más grandes, a menudo por órdenes de magnitud.

La siguiente tabla ilustra los tamaños típicos para ML-DSA en un nivel de seguridad post-cuántico de 128 bits en comparación con sus homólogos clásicos como ECDSA de 256 bits:

| Algoritmo | Tamaño de clave pública (Bytes) | Tamaño de clave privada (Bytes) | Tamaño de signature (Bytes) |
|---|---|---|---|
| ML-DSA-87 (Dilithium) | 2.592 | 4.896 | 4.627 |
| ECDSA (256-bit) | 32 | 32 | 65 |

**Como se muestra, las signature ML-DSA pueden ser más de 70 veces más grandes que los equivalentes de ECDSA, y las claves públicas más de 80 veces más grandes.**

Otras familias de PQC agravan esto: los esquemas basados en hash como SPHINCS+ pueden producir signature de hasta 41 KB, mientras que incluso las variantes de red optimizadas en tamaño como FALCON siguen superando los tamaños clásicos por un múltiplo significativo.

En contextos de blockchain, estos tamaños inflados se traducen en problemas de escalado sistémico. Las signature más grandes abultan las transacciones individuales, reduciendo las transacciones por segundo (TPS) a medida que los bloques se llenan más rápido y requieren más tiempo para su validación. Esto también tensiona la comunicación entre pares (P2P), aumentando las demandas de ancho de banda y los retrasos en la propagación, lo que puede aumentar el riesgo de bifurcaciones de red o bloques huérfanos en mecanismos de consenso como el proof-of-work. Los requisitos de almacenamiento auch se ven afectados, lo que conlleva mayores costes operativos

de los nodos y barreras para la participación, especialmente para usuarios o validadores con recursos limitados.

**Estos desafíos de escalado tendrán que ser abordados por todas las blockchains en el futuro. Bitcoin, por ejemplo, tendrá mucho menos de 1 TPS si no se aumenta el tamaño máximo de bloque.**

# Arquitectura de Quantus Network

## Primitivas criptográficas post-cuánticas

Quantus Network emplea primitivas **PQC estandarizadas por el NIST** para garantizar la seguridad de las transacciones y las comunicaciones de red frente a las amenazas cuánticas. En el núcleo de la integridad de las transacciones se encuentra **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, anteriormente conocido como CRYSTALS-Dilithium), un esquema de firma basado en redes seleccionado por su equilibrio entre seguridad, eficiencia y facilidad de implementación. **ML-DSA aprovecha la dureza de problemas** como Learning With Errors (LWE) und Short Integer Solution (SIS) sobre redes de módulos, proporcionando una resistencia robusta tanto a los ataques clásicos como a los cuánticos, incluidos los del algoritmo de Shor.

Para las firmas de transacciones, **Quantus integra ML-DSA-87**, el conjunto de parámetros que ofrece el nivel de seguridad más alto (NIST Security Level 5, equivalente a una seguridad clásica de 256 bits y cuántica de 128 bits) para **proteger contra posibles avances criptoanalíticos en problemas de redes**. Esta elección prioriza la precaución, ya que la criptografía de redes es relativamente nueva y está menos probada que los esquemas clásicos. Los parámetros más grandes mitigan los riesgos de posibles avances en el criptoanálisis de redes, que aún dejarían los tamaños de clave más pequeños como objetivos más fáciles.

### Alternativas

ML-DSA fue seleccionado frente a alternativas como FN-DSA (Falcon) debido a:

- La mayor complejidad de implementación de FN-DSA (por ejemplo, requiere operaciones de punto flotante, que no son amigables para blockchain)
- La falta de generación de claves deterministas en su especificación
- Su estado no finalizado en el momento del desarrollo

Las opciones basadas en hash como SLH-DSA fueron descartadas por sus tamaños de firma aún mayores (superando los 17 KB). La agilidad criptográfica (poder intercambiar diferentes esquemas de firma) está integrada en Substrate, por lo que es relativamente fácil añadir estas alternativas en una fecha futura, si las circunstancias lo exigen.

Si bien ML-DSA-87 da como resultado claves y signature más grandes, estas son manejables en la red de etapa temprana de Quantus, donde el almacenamiento aún no

es un cuello de botella, y las optimizaciones futuras como las wormhole addresses mediante pruebas de conocimiento cero abordarán el escalado.

Para detalles técnicos sobre la implementación, consulte QIP-0006.

### LibP2P

**Quantus Network asegura las comunicaciones entre nodos peer-to-peer (P2P) utilizando una combinación de ML-DSA para la autenticación y ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, anteriormente CRYSTALS-Kyber) para el cifrado**.

Esta integración extiende la PQC a la pila de red libp2p, modificando los componentes principales para la resistencia cuántica: utilizando signature ML-DSA-87 para la identidad de los pares y ML-KEM-768 para la seguridad del transporte (extendiendo el apretón de manos Noise con un mensaje KEM adicional para secretos compartidos resistentes a la computación cuántica).

La capa P2P a menudo se descuida en el análisis de seguridad cuántica. La autenticación de los pares es importante, pero lo peor que un atacante podría hacer a nivel de pares es suplantar a un nodo y enviar mensajes inválidos, lo que podría resultar en una denegación de servicio. Este ataque ya está mitigado por el hecho de que los nodos generalmente no son de confianza en el modelo de blockchain y los nodos pueden cambiar fácilmente sus claves si se detecta el ataque. Del mismo modo, descifrar las comunicaciones P2P produce beneficios limitados para el atacante (por ejemplo, rastrear las rutas de las transacciones, mitigado por proxies o Tor), y la mayoría de los datos se hacen públicos on-chain de todos modos.

**No obstante, asegurar cuánticamente la capa P2P protege contra la escucha, los ataques de hombre en el medio y el descifrado cuántico, garantizando que el cotilleo de los nodos, la propagación de bloques y otras interacciones de red sigan siendo confidenciales y a prueba de manipulaciones en el futuro previsible**.

Para detalles técnicos sobre la implementación, consulte QIP-0004.

## Escalado de la PQC

Para abordar los desafíos de escalado inherentes a la criptografía post-cuántica, **Quantus Network introduce un innovador esquema de firma post-cuántica agregada llamado "Wormhole Addresses"**. Este sistema aprovecha los zero-knowledge proofs (ZKPs) generados a través del sistema de prueba Plonky2 (básicamente STARKs) para mover la verificación del saldo fuera de la cadena, permitiendo que la cadena verifique una única prueba compacta sin procesar signature individuales.

**Las Wormhole Addresses permiten la verificación de un gran número de transacciones con una sola prueba**, siendo los inputs públicos (por ejemplo, nullifiers, raíz de almacenamiento, direcciones de salida y cantidades) el principal factor limitante. Esto reduce las demandas de almacenamiento por transacción amortizadas a **aproximadamente 256 bytes adicionales por transacción, mucho menos que cualquier esquema de firma PQC conocido**.

La seguridad cuántica del esquema se deriva del uso de la función hash segura Poseidon2 para los compromisos a través de FRI (Fast Reed-Solomon Interactive Oracle Proofs), en lugar de los emparejamientos de curvas elípticas vulnerables a la computación cuántica comúnmente utilizados en los SNARKs.

Además, los secretos de autenticación se ocultan tras Poseidon2. Dado que las funciones hash seguras solo se ven debilitadas cuadráticamente por el algoritmo de Grover, no rotas, las pruebas de preimagen de hash pueden servir como signature post-cuánticas ligeras en contextos ZK, de forma similar a los esquemas basados en hash como SPHINCS+.

### Flujo de Cliente / Prover

Los usuarios generan una dirección demostrablemente no gastable haciendo un doble hash de una sal (salt) concatenada con un secreto:

```
H(H(salt|secret))
```

Esta construcción evita los falsos positivos (por ejemplo, confundir una clave pública de un solo hash con una dirección no gastable) porque en Substrate (y en general) las direcciones de blockchain son el hash único de una clave pública, que se deriva de la clave privada mediante alguna operación algebraica, no mediante un hash seguro. Por lo tanto, la seguridad de la construcción se reduce a encontrar la preimagen de una preimagen de un hash seguro. Los tokens enviados a esta dirección se queman efectivamente. No se pueden gastar porque no existe ninguna clave privada para la dirección que los recibió. Por lo tanto, estas monedas pueden volver a acuñarse (re-minted) sin inflar la oferta.

Para cada transferencia, se crea un objeto de almacenamiento TransferProof, que contiene detalles como un recuento de transferencia global único. La billetera del usuario genera una prueba de almacenamiento Merkle-Patricia-Trie (MPT) desde la raíz de almacenamiento de la cabecera de un bloque reciente hasta la hoja de este TransferProof.

Se calcula un nullifier:

```
H(H(salt | secret | global_transfer_count))
```

Para evitar el doble gasto, con el secreto derivado de forma determinista de la semilla de la billetera para su retención.

### Flujo del Agregador

Cualquier parte (cliente, minero o tercero) puede agregar múltiples pruebas utilizando la recursión de Plonky2, formando un árbol de pruebas donde cada prueba madre es una verificación de las pruebas hijas, con los inputs públicos de las pruebas hijas agregados:

- los nullifiers pasan sin cambios
- las direcciones de salida se deduplican
- los hashes de los bloques se demuestran vinculados y luego se descartan todos menos el más reciente
- se suman las cantidades para las direcciones de salida duplicadas Esta recursión admite la agregación jerárquica, reduciendo drásticamente los datos on-chain.

### Flujo de Cadena / Verificador

**La red verifica la prueba agregada comprobando:**

- el hash del bloque está on-chain y es reciente
- la unicidad del nullifier (para evitar el doble gasto)
- la validez de la prueba

**El circuito ZK impone:**

- la corrección de la prueba de almacenamiento
- la precisión del cálculo del nullifier
- la no gastabilidad de la dirección
- la coincidencia del saldo entre los inputs y los outputs
- la vinculación de la cabecera del bloque

**Plonky2 fue seleccionado por las siguientes razones:**

- ya auditado

- post-cuántico
- sin configuración de confianza (trusted setup)
- generación de pruebas/verificación eficiente
- agregación de pruebas fluida
- implementación nativa en Rust
- compatible con el entorno no-std de Substrate

### Los aspectos más destacados del rendimiento incluyen:

**Pruebas recursivas en 170 milisegundos y tamaños compactos** (100 KB por prueba agregada), lo que permite ganancias masivas de rendimiento.

En un caso óptimo con bloques de 5 MB y todas las transacciones dirigidas a la misma salida, **las Wormhole Addresses podrían empaquetar ~153.000 transacciones en un solo bloque** (4,9 MB / 32 bytes por nullifier), una mejora de 223 veces respecto a las ~685 transacciones ML-DSA sin procesar (5 MB / 7,3 KB cada una).

### Notas de seguridad

Los riesgos potenciales incluyen errores de inflación por implementaciones defectuosas del circuito/verificación, aunque esto sería económicamente detectable si las monedas reacuñadas superan los saldos de las direcciones de envío cero. Los usuarios pueden demostrar opcionalmente que una dirección es un wormhole publicando el primer hash sin revelar el secreto. Las transacciones de verificación no están firmadas, por lo que la denegación de servicio mediante transacciones fallidas debe mitigarse de forma no financiera. Los cálculos de la oferta de tokens se mantienen, ya que las reacuñaciones aparecen como nuevas monedas pero mantienen las garantías de oferta máxima mediante las quemas.

Para más detalles técnicos sobre la implementación, consulte QIP-0005.

## Mecanismo de consenso

**Quantus Network utiliza un algoritmo de consenso Proof-of-Work (PoW) que preserva las propiedades deseables del algoritmo de consenso de Bitcoin al tiempo que mejora la compatibilidad con los sistemas de prueba ZK al sustituir SHA-256 por Poseidon2**.

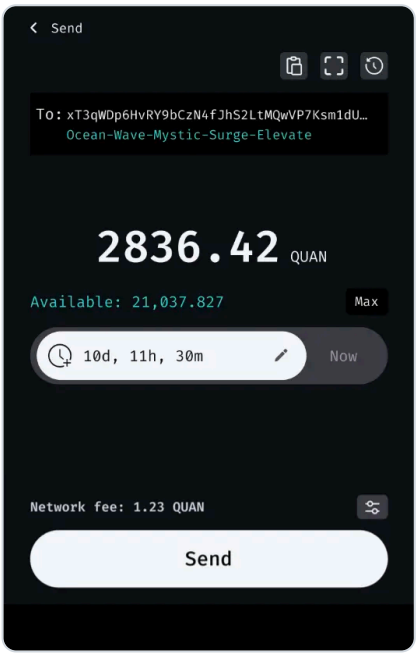
Es importante destacar que este cambio no se realiza por seguridad cuántica. Las funciones hash criptográficas como SHA-256 se ven debilitadas pero no destruidas por los algoritmos cuánticos, especialmente el de Grover. Algunos esquemas de firma post-cuántica utilizan hashes seguros como bloque de construcción por esta razón.

Poseidon2 es un refinamiento de la función hash Poseidon. La creación de SNARKs o STARKs para cálculos que involucran funciones hash tradicionales como SHA-256 a menudo requiere casi 100 veces el número de puertas en comparación con el uso de Poseidon, que se basa totalmente en funciones algebraicas sobre elementos de campo, en lugar de operaciones a nivel de bits. Utilizamos el campo Goldilocks tanto para Poseidon2 como para Plonky2 para maximizar la eficiencia.

# Preservación de la riqueza

**Hay muchos riesgos en la gestión de las claves de las criptomonedas. La mayoría de ellos son evitables. Quantus Network integra la facilidad de uso en la propia cadena, permitiendo a los no expertos realizar transacciones con tranquilidad.**

## Transacciones reversibles

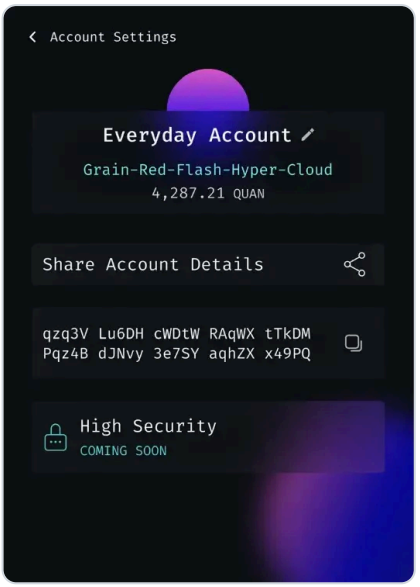



**Quantus Network ofrece transacciones reversibles configurables por el usuario, lo que permite a los remitentes establecer una ventana de tiempo durante la cual pueden cancelar las transferencias salientes, mejorando la disuasión del robo y la corrección de errores sin sacrificar la irreversibilidad central de la blockchain.** Aprovechando un "scheduler pallet" de Substrate modificado que utiliza marcas de tiempo para retrasos intuitivos, el sistema permite a los clientes programar transferencias a través de una interfaz sencilla, mostrando cuentas atrás en las billeteras tanto para el remitente (con un botón de cancelación) como para el destinatario (indicando la finalización si no se cancela). Esto equilibra la finalidad rápida para el comercio con la flexibilidad para los usuarios preocupados por cometer errores o que deseen realizar un depósito de buena fe sin un servicio de custodia.

**Las transacciones reversibles forman un potente bloque de construcción para nuevos protocolos de seguridad, manteniendo al mismo tiempo la descentralización mediante la ejecución on-chain.**

Para más detalles técnicos, consulte QIP-0009.

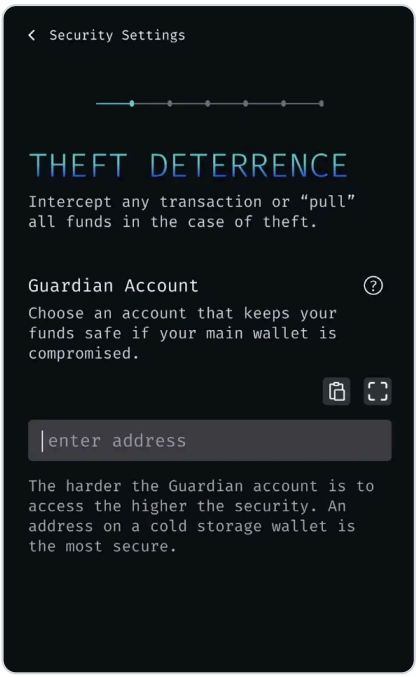
## Check-Phrases




Quantus Network introduce las “check-phrases”, una suma de comprobación legible por humanos y criptográficamente segura para direcciones de blockchain y otros datos que requieren verificación humana. **Al hacer un hash de la dirección para generar una secuencia corta de palabras memorables de la lista mnemónica BIP-39, las check-phrases permiten comprobaciones de integridad rápidas y sin errores, protegiendo contra errores tipográficos, manipulaciones y ataques como el address poisoning**. Esta herramienta permite a los usuarios verificar direcciones con confianza durante las transferencias sin depender de pantallas truncadas o sumas de comprobación débiles. Se utiliza una función de derivación de claves de 50.000 iteraciones para garantizar que la creación de una tabla arcoíris para unas sumas de comprobación dadas sea muy costosa. Por supuesto, para transacciones grandes, los usuarios deben seguir comprobando manualmente cada letra de la dirección para verificar su exactitud.

Para más detalles técnicos, consulte QIP-0008.

## Cuentas de alta seguridad




Quantus Network ofrece la posibilidad de actualizar cualquier cuenta a una "cuenta de alta seguridad" que impone periodos de reversión obligatorios en todas las transferencias salientes, permitiendo que una cuenta "guardián" (guardian) designada, como una billetera de hardware, un multisig o incluso un tercero de confianza elegido por el usuario, cancele exclusivamente transacciones sospechosas durante el periodo de reversión, enviando los fondos al guardián en lugar de al remitente o al receptor. Esta característica permanente y opcional se basa en las transferencias reversibles, donde los usuarios especifican el retraso y el interceptor tras la activación, evitando que los ladrones lo desactiven.

El interceptor puede ser a su vez otra cuenta de alta seguridad con su propio guardián, lo que permite jerarquías componibles donde cada guardián tiene permisos superiores a la cuenta que protege. Este diseño imita las reversiones ordenadas por los tribunales de las finanzas tradicionales, pero con el control del usuario. Equilibra la seguridad y la comodidad para las cuentas de alto valor, dando tiempo para detectar y responder a actividades no autorizadas sin comprometer la finalidad de la blockchain para los flujos legítimos.

Para más detalles técnicos, consulte QIP-0011.

## Recuperación de claves

Muchas fortunas en cripto han ido a la tumba con sus dueños. Quantus Network ofrece una forma sencilla de especificar una dirección de recuperación que puede retirar sus fondos en cualquier momento, con sujeción a un retraso fijo. Durante este tiempo, el propietario puede denegar la recuperación si tiene acceso a la clave. Esta característica permite la supervivencia: los usuarios tienen un testamento on-chain sin necesidad de tribunales ni herencias.

## HD-Lattice

Las billeteras jerárquicas deterministas (HD) son el estándar de la industria para las blockchains, permitiendo a los usuarios hacer una copia de seguridad de una sola frase semilla para todas las claves, mejorando la seguridad y la comodidad frente a las copias de seguridad manuales por acción.

Adaptar esto a esquemas de red como Dilithium implica dos desafíos:

- Los outputs de HMAC-SHA512 no pueden formar directamente claves privadas de red, que requieren polinomios de "buena base" mediante muestreo de rechazo.
- La derivación de claves no endurecida (non-hardened) se basa en la adición de curvas elípticas, ausente en las redes (las claves públicas no están cerradas bajo ninguna operación algebraica).

Quantus Network aborda el primer problema utilizando el output del HMAC como entropía para construir de forma determinista la clave privada, no como la clave privada en sí misma. El segundo problema es menos crítico y sigue siendo una cuestión de investigación abierta si la criptografía de redes puede adaptarse para abordarlo.

Para más detalles técnicos, consulte QIP-0002.

# Tokenomics y Gobernanza

Quantus Network existe en un entorno cambiante, y no podemos asumir que lo haremos todo bien al primer intento. Por esta razón, elegimos un punto de partida sencillo y permitimos que el sistema de gobernanza realice cambios a medida que se adquiere nueva información. Este diseño convierte a la blockchain en una entidad viva que puede adaptarse a su entorno a voluntad. En particular, el proceso de gobernanza de Substrate permite cambios profundos en la chain con una coordinación mínima entre los diversos ejecutores de nodos.

## Recompensas de bloque

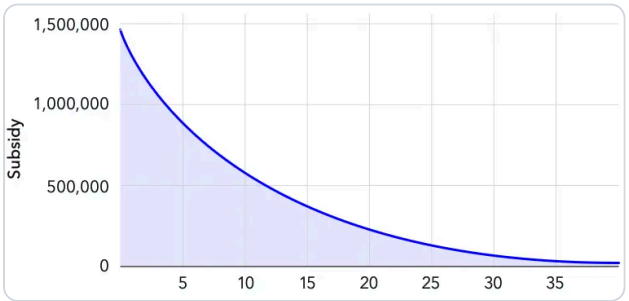
Quantus Network emplea un modelo de tokenomics sencillo que imita al de Bitcoin. Hay un suministro máximo de 21.000.000 de monedas y una heurística simple determina la recompensa de cada bloque.

```
block_reward = (max_supply-current_supply) / constant
```

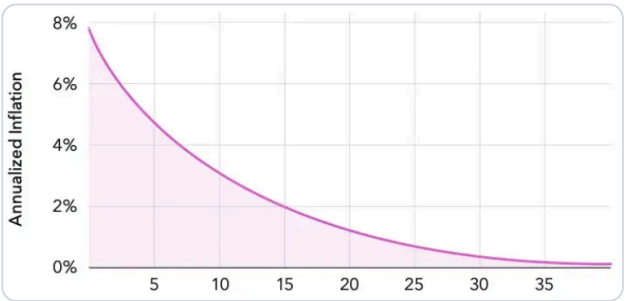
Esta heurística forma una curva de decaimiento exponencial suave, ya que la block_reward contribuye al current_supply, lo que reduce la block_reward calculada en el siguiente bloque.

Cualquier quema de comisiones o de otro tipo reduce el current_supply y se convierte esencialmente en parte del presupuesto para las recompensas de bloque. La constante se elige de modo que, en ausencia de quemas, el 99% de las monedas se emitan en unos 40 años.

**Recompensas de bloque / Año**




**Inflación / Año**



## Asignación de inversores

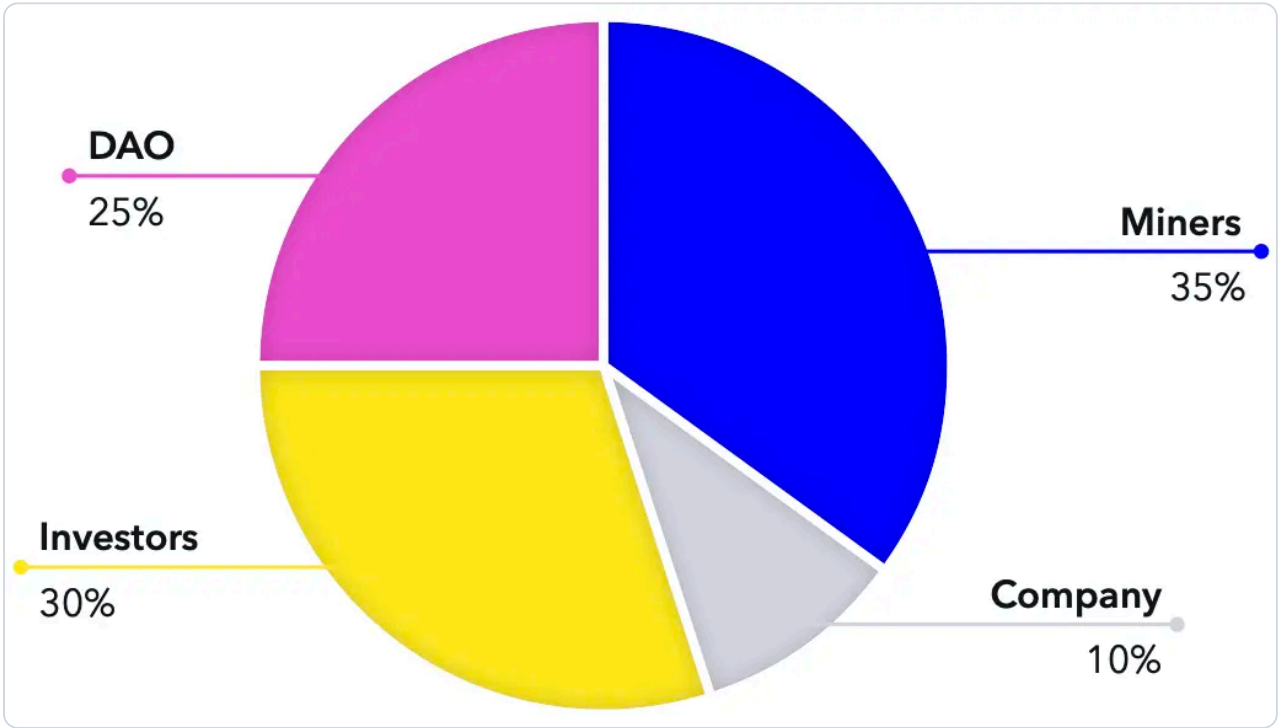
Quantus Network se construyó con la ayuda de inversores ángeles que asumieron un gran riesgo al financiarla. Para evitar los excedentes de oferta que crean los bloqueos de los inversores (investor-lockups), estamos haciendo que todos los inversores, públicos y privados, tengan liquidez desde el primer día. Esta asignación será el único "pre-mine". Todos los demás tokens tendrán que ser minados para existir. Dependiendo del éxito de las ventas públicas, esta porción representará el 20-30% del suministro total.

## Asignación de la empresa

Para compensar al equipo por asumir el riesgo de construir nueva tecnología sin promesa de éxito, dividiremos las recompensas de bloque en dos mitades. La primera mitad irá al minero. Durante aproximadamente cuatro años, la segunda mitad irá a la empresa. Esto da un calendario de consolidación (vesting) de facto de aproximadamente el 10% del suministro total a la empresa. Durante este tiempo, los mineros reciben la misma cantidad de monedas recién acuñadas.

Después de ese punto, la porción de las recompensas de bloque de la empresa se redirigirá a una tesorería gobernada por los poseedores de tokens, formando esencialmente una DAO.

**Asignación aproximada del suministro**



## Comisiones de transacción

Las transacciones estándar tendrán una comisión que va a los mineros, proporcionando un incentivo para incluir transacciones. Las transacciones revertidas de cuentas de alta seguridad tendrán una comisión basada en el volumen del 1% que se divide, yendo la mitad al minero y la otra mitad siendo quemada, yendo al presupuesto de seguridad futuro. Las transacciones que pasan por el sistema de agregación zk también estarán sujetas a una comisión basada en el volumen del 0,1%, que se repartirá entre el minero, el agregador de pruebas y una quema.

## Actualizaciones sin bifurcación (Forkless Upgrades)

Quantus Network admite actualizaciones "sin bifurcación" a través de las actualizaciones del runtime de Substrate, lo que permite que la lógica central de la blockchain (el "runtime") evolucione sin bifurcaciones duras (hard forks) que podrían interrumpir la red o dividir a la comunidad. Esto se logra a través de referéndums de gobernanza on-chain, donde las propuestas aprobadas activan un intercambio de runtime, sustituyendo esencialmente el blob de código WASM existente por uno nuevo en un solo bloque, garantizando la continuidad del estado y las operaciones. Esta ruta de actualización minimiza el tiempo de inactividad y los riesgos, permitiendo a la comunidad refinar iterativamente el protocolo.

## Sistema de gobernanza

Quantus Network hereda su marco de gobernanza del sistema OpenGov de Polkadot a través de Substrate. Los poseedores de tokens participan mediante el voto por convicción (conviction voting), en el que aceptan bloquear sus activos durante periodos variables para ampliar el peso de su voto. Esta ampliación puede ir desde 1x (sin bloqueo) hasta 6x (bloqueo máximo). Este diseño fomenta la alineación a largo plazo al vincular la influencia con el compromiso.

Las propuestas se categorizan en múltiples vías de votación llamadas "origins". Cada origin tiene parámetros adaptados, como umbrales de aprobación (por ejemplo, supermayoría para cambios de alto impacto), depósitos mínimos para disuadir el spam, periodos de preparación/ejecución y plazos de decisión para evitar el estancamiento. Este diseño de múltiples vías permite el procesamiento paralelo de diversos referéndums, desde gastos rutinarios de tesorería hasta actualizaciones críticas del runtime.

El Colectivo Técnico es un grupo selecto de expertos técnicos que actúa como un organismo especializado para proponer, revisar o incluir en una lista blanca asuntos

técnicos urgentes, agilizándolos a través de una vía dedicada mientras se mantiene la supervisión de la comunidad.

Quantus adopta este sistema sin modificaciones, pero comienza con una configuración minimalista para evitar la complejidad en sus etapas iniciales. Inicialmente, solo está activa la vía del Colectivo Técnico, que se utilizará para decisiones vinculantes y de alto privilegio, como actualizaciones del protocolo o ajustes de parámetros.

Más adelante introduciremos la vía de voto comunitario no vinculante para medir el sentimiento sobre temas no ejecutables, como sugerencias de características o encuestas del ecosistema. Este sistema pasará a ser vinculante cuando la empresa entregue la red a la DAO.

Este enfoque gradual permite que la red evolucione orgánicamente a través de futuras votaciones de gobernanza sin cargar a los usuarios con una complejidad innecesaria al principio.

# Hoja de ruta

## Heisenberg Inception

DICIEMBRE 2024

**Financiación asegurada, Substrate elegido**

## Resonance Alpha

JULIO 2025

**Testnet pública, firmas Dilithium, transacciones reversibles**

## Schrödinger Beta

OCTUBRE 2025

**Características completas, listo para auditoría**

## Dirac Beta

NOVIEMBRE 2025

**PoW cambiado a Poseidon2, auditorías abordadas**

## Planck Beta

ENERO 2026

**Cuentas de alta seguridad, multising, billetera de hardware**

## Bell Mainnet

Q1 2026

**Lanzamiento de la Mainnet**

## Fermi Upgrade

Q2 2026

**Agregación ZK**

## Riesgos

La construcción de Quantus Network conlleva riesgos inherentes.

- **Problemas de implementación:** Los fallos en la lógica del software pueden causar fallos graves incluso en los sistemas mejor diseñados.
- **Problemas de selección de algoritmos del NIST:** Posibles fallos o puertas traseras en los estándares post-cuánticos seleccionados (por ejemplo, ML-DSA, ML-KEM) que podrían surgir tras la estandarización. En el peor de los casos, tales fallos permitirían a un atacante falsificar signature derivando una clave privada de la pública, lo que representaría un modo de fallo catastrófico de la chain. Si tales fallos se hicieran públicos, Quantus Network podría actualizarse a un nuevo algoritmo, pero si tales fallos se explotan con moderación, es posible que nunca se descubran.
- **Plazos de la computación cuántica:** Los avances cuánticos podrían llegar mucho más tarde de lo previsto, retrasando la necesidad de PQC; por el contrario, el desarrollo secreto (por ejemplo, por parte de los gobiernos) podría dar lugar a amenazas repentinas si la comunidad blockchain no se actualiza con rapidez.
- **Otras consideraciones:** Barreras generales de adopción, incertidumbres regulatorias en las finanzas/blockchain y la volatilidad inherente de los ecosistemas cripto.

## Cierre

QUANTUS

Creemos en el poder de los protocolos abiertos, el proof-of-work y la propiedad soberana. La aplicación Quantus Network, disponible para escritorio y móviles, permite a los usuarios almacenar activos digitales, minar nuevos bloques y participar en un futuro financiero más justo sin intermediarios.

Estamos comprometidos con la transparencia, la privacidad y el empoderamiento de las personas a través de herramientas de autocustodia seguras.