quantus

dinero cifrado y seguro en el sentido cuántico

PUBLICADO
21 de marzo de 2026

VERSIÓN
0.3.3

CLASIFICACIÓN
public

Este whitepaper se ofrece únicamente con fines informativos y no constituye una oferta de venta, una solicitud de oferta de compra ni una recomendación sobre ningún valor, inversión o producto financiero. Los lectores deben realizar su propia diligencia debida y consultar a profesionales cualificados antes de tomar decisiones de inversión. Quantus Network no ofrece declaraciones ni garantías sobre la exactitud o integridad de la información aquí contenida.

CONTENIDO

01

introducción

la amenaza cuántica

Las blockchains tradicionales enfrentan una amenaza existencial por los ordenadores cuánticos criptográficamente relevantes (CRQC). Los fundamentos criptográficos de las blockchains dependen de la dificultad del problema del logaritmo discreto (DLP), y los algoritmos cuánticos, en particular el de Shor, pueden resolver el DLP exponencialmente más rápido que los ordenadores clásicos. Esta vulnerabilidad podría permitir a adversarios cuánticos derivar claves privadas a partir de claves públicas, lo que les permitiría falsificar transacciones y descifrar datos financieros sensibles.

> sin actualizaciones proactivas resistentes a la computación cuántica, la economía cripto de billones de dólares arriesga una desvalorización repentina por tales ataques.

propuesta de valor única

Nombrada por la palabra latina que significa «cuánto», Quantus Network permite dinero privado escalable y seguro en el sentido cuántico. Quantus no es una plataforma general de contratos inteligentes. Como un restaurante con unos pocos platos muy perfeccionados, Quantus ofrece:

— Firmas post-cuánticas para todas las transacciones

— Firmas y cifrado post-cuánticos (ML-DSA y ML-KEM) para asegurar conexiones entre pares

— Pruebas de conocimiento cero post-cuánticas para escalar

— Cuentas de alta seguridad para disuadir el robo y permitir recuperación de errores

— Frases de comprobación legibles para verificación sencilla de direcciones

La decisión de centrarse en dinero privado escalable y seguro en el sentido cuántico surge de la amenaza que los CRQC plantean al sector y de la incapacidad de Bitcoin para abordar estos retos.

02

la amenaza cuántica para la blockchain

fundamentos de la computación cuántica

Los ordenadores cuánticos aprovechan principios como la superposición y el entrelazamiento para realizar cálculos intratables para máquinas clásicas. A diferencia de los bits clásicos, que son 0 o 1, los qubits pueden existir en múltiples estados a la vez, permitiendo 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 hardware cuántico socavan los supuestos de seguridad de la mayor parte de la criptografía de clave pública.

El algoritmo de Shor, presentado en 1994 por Peter Shor, ofrece un método en tiempo polinómico para factorizar enteros grandes y resolver el problema del logaritmo discreto en un ordenador cuántico. Explota las transformadas cuánticas de Fourier (QFT) para hallar el periodo de una función, permitiendo invertir eficientemente las funciones trampilla que sustentan esquemas como RSA o la criptografía de curvas elípticas (ECC). Para las finanzas en blockchain, esto significa que un atacante con un ordenador cuántico suficientemente potente (estimado en ~2.000

qubits lógicos [6][7][8][9]) podría derivar claves privadas a partir de claves públicas en tiempo polinómico $O(n^3)$: una aceleración extrema que deja obsoletos los sistemas vulnerables de la noche a la mañana. [1]

El algoritmo de Grover, propuesto por Lov Grover en 1996, ofrece una aceleración cuadrática para búsquedas no estructuradas, reduciendo el tiempo de búsqueda de $O(n)$ a $O(\sqrt{n})$ operaciones. Aunque no es tan devastador como Shor para la criptografía asimétrica, Grover afecta primitivas simétricas como funciones hash y el cifrado AES, reduciendo efectivamente a la mitad el nivel de seguridad (p. ej., una clave de 256 bits se comporta como 128 bits frente a ataques cuánticos). Este ataque se mitiga duplicando los bits de seguridad en lugar de cambiar el esquema criptográfico. Además, la aceleración cuadrática de Grover es poco práctica por sus altos requisitos de qubits y puertas, exigiendo miles de millones de operaciones secuenciales con paralelización limitada, lo que la hace inviable para inversiones en el mundo real incluso con hardware futuro. [2]

cuatro categorías de amenaza

01 - falsificar firmas digitales

El algoritmo de Shor amenaza directamente las firmas basadas en ECC usadas en la mayoría de las blockchains (p. ej., la curva secp256k1 de Bitcoin), permitiendo a adversarios suplantar usuarios y autorizar transacciones fraudulentas. Tal capacidad

supondría un fallo crítico de la característica más básica de una blockchain.

02 - falsificar pruebas falsas en sistemas de conocimiento cero

Muchas pruebas de conocimiento cero, como las de zk-SNARKs para finanzas centradas en la privacidad, dependen de la dificultad del logaritmo discreto mediante emparejamientos de curvas elípticas para los compromisos. Shor podría permitir crear pruebas inválidas que parezcan válidas, lo que permitiría a un atacante acuñar monedas nuevas o falsificar el estado de las capas 2 (L2).

03 - descifrar 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 comunicaciones p2p en protocolos financieros, revelando detalles patrimoniales sensibles y permitiendo robos dirigidos.

04 - invertir funciones hash

El algoritmo de Grover podría acelerar ataques de preimagen sobre hashes como SHA-256, usados en prueba de trabajo y generación de direcciones, pero es la amenaza menos preocupante. Muchos esquemas criptográficos post-cuánticos incorporan construcciones basadas en hash, ya que los hashes se consideran suficientemente seguros con un digest lo bastante grande.

retos de escalado en la criptografía post-cuántica

Aunque la criptografía post-cuántica (PQC) ofrece protecciones esenciales frente a amenazas cuánticas, introduce obstáculos de escalado importantes debido al diseño inherente de estos algoritmos. A diferencia de los esquemas de curvas elípticas, que se apoyan en estructuras matemáticas compactas, las primitivas PQC requieren parámetros mayores para mantener la seguridad frente a adversarios clásicos y cuánticos. Ello produce claves públicas, claves privadas y firmas notablemente mayores, a menudo en órdenes de magnitud. La siguiente tabla ilustra tamaños típicos de ML-DSA a un nivel de seguridad post-cuántica de 128 bits frente a equivalentes clásicos como ECDSA de 256 bits: [10]

ALGORITMO	CLAVE PÚBLICA	CLAVE PRIVADA	FIRMA
ML-DSA-87 (Dilithium)	2,592 bytes	4,896 bytes	4,627 bytes
ECDSA (256-bit)	32 bytes	32 bytes	65 bytes

Tamaños a nivel de seguridad post-cuántica de 128 bits. Fuente: Open Quantum Safe Project [10]

Como se ve, las firmas ML-DSA pueden ser más de 70 veces mayores que las equivalentes ECDSA, y las claves públicas más de 80 veces mayores. Otras familias PQC lo agravan: esquemas

basados en hash como SPHINCS+ pueden producir firmas de hasta 41 KB, mientras que variantes lattice optimizadas en tamaño como FALCON siguen superando los tamaños clásicos en un múltiplo significativo.

En contextos blockchain, estos tamaños inflados se acumulan en problemas de escalado sistémico. Las firmas mayores hinchan las transacciones individuales, reduciendo las transacciones por segundo (TPS) al llenarse los bloques más rápido y requerir más tiempo de validación. También tensan la comunicación peer-to-peer (P2P), aumentando el ancho de banda y los retrasos de propagación, lo que puede aumentar el riesgo de bifurcaciones u bloques huérfanos en mecanismos de consenso como la prueba de trabajo. Los requisitos de almacenamiento también se ven afectados, con mayores costes operativos de los nodos y barreras a la participación, especialmente para usuarios o validadores con recursos limitados.

> **NOTA**
>
> Estos retos de escalado tendrán que abordarlos todas las blockchains en el futuro. Bitcoin, por ejemplo, tendrá mucho menos de 1 TPS si no se aumenta el tamaño máximo del bloque.

03

la crisis de la migración

el problema de coordinación

La cultura conservadora de Bitcoin resiste los cambios de protocolo. Cualquier mejora PQC exigiría consenso sobre cuestiones polémicas como plazos de migración, posible decomiso de monedas y aumentos del tamaño de bloque. Incluso si la comunidad acordara, cada usuario tendría que migrar sus monedas a nuevas direcciones seguras en el sentido cuántico. La migración exige acción de todos los titulares de cripto, muchos de los cuales han perdido acceso a sus monederos o ignoran la amenaza.

Estos problemas existen en toda blockchain pública, pero son singularmente difíciles para Bitcoin por su falta de liderazgo claro y su filosofía de osificación técnica.

el problema de las monedas perdidas

Se estima que entre 250.000 y 500.000 millones de dólares en Bitcoin son inaccesibles de forma permanente por claves perdidas, titulares fallecidos o monederos olvidados. [3] Estas monedas no pueden migrarse y actúan como recompensa pública por crear un ordenador cuántico criptográficamente relevante (CRQC). Los atacantes cuánticos derivarán claves privadas de claves públicas no

migradas y probablemente volcarán miles de millones de dólares en BTC al mercado.

> la única solución técnica exige un plazo estricto que congele las monedas no migradas: una imposibilidad política.

Sin tal plazo, el resultado será que las monedas no migradas se roben y vendan, hundiendo el mercado y destruyendo la confianza en la red.

el problema del calendario de migración

Las firmas post-cuánticas son entre 20 y 80 veces mayores que las firmas actuales de Bitcoin. Sin cambios arquitectónicos fundamentales, el rendimiento de Bitcoin colapsará a una fracción de su capacidad ya limitada.

Suponiendo que Bitcoin resuelve los retos políticos y técnicos, la migración en sí llevaría meses o años. Cada titular debe enviar al menos una transacción para mover fondos a una dirección segura en el sentido cuántico. Muchos enviarán primero transacciones de prueba. Con firmas PQC hinchadas asfixiando el rendimiento, la red enfrenta una cola que dura meses o años mientras las monedas vulnerables al quantum siguen expuestas.

> **LA RESPUESTA DE QUANTUS**

> Estos retos acumulados hacen extraordinariamente difícil añadir seguridad cuántica a cadenas existentes. Quantus Network lo evita integrando la seguridad cuántica en la cadena desde el primer día.

04

arquitectura de quantus network

fundamentos

Quantus Network está construido sobre Substrate, un SDK de blockchain desarrollado por Parity Technologies, el equipo detrás de Ethereum y Polkadot. Substrate es altamente modular, lo que permite sustituir componentes fácilmente para centrarnos en lo que hace único a Quantus.

Quantus mejora Substrate:

— Añadiendo soporte para esquemas de firma post-cuánticos

— Actualizando la seguridad de la red p2p a post-cuántica

— Añadiendo reversibilidad de transacciones controlada por el usuario

— Haciendo la base de datos compatible con zk alineando todos los tipos de datos con límites de elementos de campo

primitivas criptográficas post-cuánticas

Quantus Network emplea PQC estandarizada por el NIST para garantizar la seguridad de transacciones y comunicaciones de red frente a amenazas cuánticas. En el núcleo de la integridad de las transacciones está **ML-DSA** (Algoritmo de firma digital basado en

módulos-retícula, antes conocido como CRYSTALS-Dilithium), un esquema de firma basado en retículos seleccionado por su equilibrio entre seguridad, eficiencia y facilidad de implementación. ML-DSA aprovecha la dificultad de problemas como Learning With Errors (LWE) y Short Integer Solution (SIS) sobre módulos reticulares, ofreciendo resistencia robusta frente a ataques clásicos y cuánticos, incluidos los del algoritmo de Shor. [4]

Para firmas de transacción, Quantus integra **ML-DSA-87**, el conjunto de parámetros con el nivel de seguridad más alto (Nivel 5 del NIST, equivalente a 256 bits clásicos y 128 bits cuánticos) para proteger frente a posibles avances en criptanálisis de retículos. Esta elección prioriza la cautela, ya que la criptografía de retículos es relativamente nueva y menos probada en combate que los esquemas clásicos. Los parámetros mayores mitigan riesgos de avances potenciales en criptanálisis de retículos, que aún dejarían tamaños de clave menores como objetivos más débiles.

alternativas consideradas

Se eligió ML-DSA frente a alternativas como FN-DSA (Falcon) por la mayor complejidad de implementación de FN-DSA (p. ej., requiere operaciones en coma flotante, poco adecuadas a blockchain), la ausencia de generación de claves determinista en su especificación y su estado no finalizado en el momento del desarrollo.

Las opciones basadas en hash como SLH-DSA no se eligieron por sus firmas aún mayores (más de 17 KB). La cripto-agilidad

(capacidad de intercambiar esquemas de firma) está integrada en Substrate, por lo que es relativamente sencillo añadir estas alternativas en el futuro si las circunstancias lo exigen.

Aunque ML-DSA-87 produce claves y firmas mayores, son gestionables en la red en fase inicial de Quantus, donde el almacenamiento aún no es un cuello de botella, y optimizaciones como direcciones wormhole mediante pruebas de conocimiento cero abordarán el escalado.

Para detalles técnicos de la implementación véase QIP-0006.

libp2p - red segura en el sentido cuántico

Quantus Network asegura las comunicaciones entre nodos peer-to-peer (P2P) combinando ML-DSA para autenticación y **ML-KEM** (Mecanismo de encapsulación de claves basado en módulos-retícula, antes CRYSTALS-Kyber) para cifrado. Esta integración extiende el PQC a la pila libp2p, modificando componentes centrales para resistencia cuántica: firmas ML-DSA-87 para identidad de pares y ML-KEM-768 para seguridad de transporte (extendiendo el handshake Noise con un mensaje KEM adicional para secretos compartidos resistentes al quantum). [5]

La capa P2P suele descuidarse en el análisis de seguridad cuántica. La autenticación de pares importa, pero lo peor que un atacante puede hacer a nivel de pares es suplantar un nodo y enviar mensajes inválidos, lo que podría causar denegación de servicio.

Este ataque ya se mitiga porque los nodos no suelen ser de confianza en el modelo blockchain y pueden cambiar de clave fácilmente si se detecta el ataque. Asimismo, descifrar comunicaciones P2P ofrece beneficios limitados al atacante (p. ej., rastrear rutas de transacción, mitigado con proxies o Tor), y la mayoría de los datos acaban siendo públicos en cadena.

No obstante, asegurar la capa P2P en el sentido cuántico protege frente a escuchas, ataques intermediarios y descifrado cuántico, garantizando que el gossip de nodos, la propagación de bloques y otras interacciones de red sigan siendo confidenciales e íntegras en el futuro previsible.

Para detalles técnicos véase QIP-0004.

escalado pqc - direcciones wormhole

Para abordar los retos de escalado inherentes a la criptografía post-cuántica, Quantus Network introduce un esquema agregado innovador de firma post-cuántica llamado **«Wormhole Addresses»**. Este sistema aprovecha pruebas de conocimiento cero (ZKP) generadas con el sistema de pruebas Plonky2 (básicamente STARKs) para llevar la verificación de saldos fuera de la cadena, permitiendo que la cadena verifique una única prueba compacta sin procesar firmas individuales. Las Wormhole Addresses permiten verificar un gran número de transacciones con una prueba, siendo los inputs públicos (p. ej., nullifiers, raíz de almacenamiento, direcciones de salida e importes) el principal factor limitador. Esto

reduce las necesidades de almacenamiento amortizadas por transacción a unos 256 bytes adicionales por transacción, mucho menor que cualquier esquema de firma PQC conocido.

La seguridad cuántica del esquema proviene del uso de la función hash segura **Poseidon2** para compromisos mediante FRI (Fast Reed-Solomon Interactive Oracle Proofs), en lugar de los emparejamientos de curvas elípticas vulnerables al quantum habituales en SNARKs.

Además, los secretos de autenticación quedan ocultos tras Poseidon2. Como las funciones hash seguras solo se debilitan cuadráticamente con el algoritmo de Grover, no se rompen; las pruebas de preimagen hash pueden servir como firmas post-cuánticas ligeras en contextos ZK, similares a esquemas basados en hash como SPHINCS+.

flujo cliente / probador

Los usuarios generan una dirección demostrablemente no gastable doble-hasheando una sal concatenada con un secreto:

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

Esta construcción evita falsos positivos (p. ej., confundir una clave pública de hash simple con una dirección no gastable) porque en Substrate (y en general) las direcciones blockchain son el hash simple de una clave pública derivada de la clave privada mediante

alguna operación algebraica, no mediante un hash seguro. La seguridad de la construcción se reduce por tanto a hallar la preimagen-de-preimagen de un hash seguro. Los tokens enviados a esta dirección se queman de facto. No pueden gastarse porque no existe clave privada para la dirección que los recibió. Estas monedas pueden acuñarse de nuevo sin inflar el suministro.

Para cada transferencia se crea un objeto de almacenamiento TransferProof, con detalles como un recuento global de transferencias único. El monedero del usuario genera una prueba de almacenamiento Merkle-Patricia-Trie (MPT) desde la raíz de almacenamiento de una cabecera de bloque reciente hasta la hoja de este TransferProof. Se calcula un nullifier para evitar doble gasto:

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

flujo del agregador

Cualquier parte (cliente, minero o tercero) puede agregar múltiples pruebas mediante la recursión de Plonky2, formando un árbol de pruebas donde cada prueba padre verifica las hijas, agregando los inputs públicos hijos:

— Los nullifiers pasan sin cambios

— Las direcciones de salida se deduplican

— Los hashes de bloque se prueban enlazados y luego se descartan salvo el más reciente

— Los importes para direcciones de salida duplicadas se suman

flujo cadena / verificador

La red verifica la prueba agregada comprobando: el hash de bloque está en cadena y es reciente, unicidad del nullifier (para evitar doble gasto) y validez de la prueba. El circuito ZK impone corrección de la prueba de almacenamiento, precisión del nullifier, no gastabilidad de la dirección, coincidencia de saldos entre entradas y salidas y enlace de cabeceras de bloque.

por qué plonky2

— Ya auditado

— Post-cuántico

— Sin trusted setup

— Prueba/verificación eficientes

— Agregación de pruebas fluida

— Implementación nativa en Rust

— Compatible con el entorno no-std de Substrate

> **RENDIMIENTO**
>
> Las pruebas recursivas terminan en 170 milisegundos con tamaños compactos (100 KB por

> prueba agregada). En un caso óptimo con bloques de 5 MB y todas las transacciones hacia 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 223x frente a ~685 transacciones ML-DSA en bruto (5 MB / 7,3 KB cada una).

notas de seguridad

Los riesgos potenciales incluyen errores de inflación por implementaciones defectuosas de circuito/verificación, aunque serían detectables económicamente si las monedas reacuñadas superan los saldos de direcciones de envío cero. Los usuarios pueden opcionalmente probar que una dirección es wormhole publicando el primer hash sin revelar el secreto. Las transacciones de verificación no están firmadas, por lo que la denegación de servicio por transacciones fallidas debe mitigarse sin medios financieros. Los cálculos de suministro de tokens se mantienen, ya que las reacuñaciones aparecen como monedas nuevas pero conservan garantías de suministro máximo mediante quemas.

Para más detalles técnicos véase QIP-0005.

mecanismo de consenso

Quantus Network usa un algoritmo de consenso Proof-of-Work (PoW) que conserva las propiedades deseables del consenso de

Bitcoin mejorando la compatibilidad con sistemas de prueba ZK sustituyendo SHA-256 por **Poseidon2**.

Importante: este cambio no se hace por seguridad cuántica. Las funciones hash criptográficas como SHA-256 se debilitan pero no se destruyen con algoritmos cuánticos, en particular Grover. Algunos esquemas de firma post-cuánticos usan hashes seguros como bloque básico por esta razón.

Poseidon2 es un refinamiento de la función hash Poseidon. Crear SNARKs o STARKs para cómputos con hashes tradicionales como SHA-256 suele requerir casi 100 veces más puertas que usando Poseidon, que se apoya por completo en funciones algebraicas sobre elementos de campo en lugar de operaciones a nivel de bit.

Usamos el **campo Goldilocks** para Poseidon2 y Plonky2. El orden del campo Goldilocks cabe en un entero sin signo de 64 bits, lo que aumenta la eficiencia sin comprometer la solidez.

05

preservación del patrimonio

Hay muchos riesgos al gestionar claves de criptomonedas. La mayoría se pueden evitar.

transacciones reversibles

Quantus Network ofrece transacciones reversibles configurables por el usuario. Los remitentes fijan una ventana temporal en la que pueden cancelar transferencias salientes. Esto disuade el robo y corrige errores sin sacrificar la finalidad. El sistema usa un pallet Substrate «scheduler» modificado con marcas de tiempo. Los monederos muestran cuentas atrás para remitente (con botón cancelar) y destinatario.

Las transacciones reversibles permiten protocolos de seguridad novedosos manteniendo la descentralización mediante aplicación en cadena.

Para más detalles técnicos véase QIP-0009.

frases de comprobación

Quantus Network introduce «check-phrases», una suma de comprobación legible y criptográficamente segura para direcciones blockchain. La dirección se hashea para generar una secuencia corta de palabras memorables de la lista mnemónica BIP-39. Las

frases de comprobación protegen frente a erratas, manipulación y ataques de envenenamiento de direcciones. Una función de derivación de clave de 50.000 iteraciones hace costosos los ataques de tabla arcoíris. Para transacciones grandes, los usuarios deben seguir verificando cada carácter de la dirección.

Para más detalle técnico véase QIP-0008.

cuentas de alta seguridad

Cualquier cuenta puede mejorarse a «cuenta de alta seguridad» con periodos de reversión obligatorios en todas las transferencias salientes. Un **guardián** designado (monedero hardware, multisig o tercero de confianza) puede cancelar transacciones sospechosas durante el periodo de reversión, enviando fondos al guardián en lugar del remitente o receptor. Esta función opt-in es permanente una vez activada, impidiendo que los ladrones la desactiven.

Los guardianes pueden encadenarse: el guardián de una cuenta de alta seguridad puede ser a su vez una cuenta de alta seguridad con su propio guardián. Esto crea jerarquías composables donde cada guardián tiene permisos superiores sobre la cuenta que protege. El diseño da tiempo a los usuarios para detectar y responder a actividad no autorizada sin comprometer la finalidad de transferencias legítimas.

Para más detalles técnicos véase QIP-0011.

recuperación de claves

Muchas fortunas 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, sujeta a un retraso fijo. Durante ese tiempo, el propietario puede denegar la recuperación si tiene acceso a la clave. Esta función permite la supervivencia: los usuarios tienen un testamento en cadena sin tribunales ni herencias formales.

hd-lattice

Los monederos jerárquicos deterministas (HD) son el estándar del sector para blockchains, permitiendo respaldar una sola frase semilla para todas las claves, mejorando seguridad y comodidad frente a copias manuales por acción. Adaptar esto a esquemas reticulares como Dilithium plantea dos retos:

— Las salidas HMAC-SHA512 no pueden formar directamente claves privadas reticulares, que son polinomios muestreados de un anillo con ciertas propiedades.

— La derivación de claves no endurecida se apoya en la suma en curvas elípticas, ausente en retículos (las claves públicas no son cerradas bajo ninguna operación algebraica).

Quantus Network aborda el primer punto usando la salida del HMAC como entropía para construir determinísticamente la clave privada, no como la clave en sí. El segundo punto es menos crítico y

sigue siendo una pregunta abierta de investigación si la criptografía reticular puede adaptarse para resolverlo.

Para más detalles técnicos véase QIP-0002.

06

tokenómica y gobernanza

Quantus Network existe en un entorno cambiante y no podemos asumir que acertaremos a la primera. Por ello elegimos un punto de partida sencillo y permitimos que el sistema de gobernanza realice cambios a medida que se obtiene nueva información. Este diseño convierte la blockchain en una entidad viva que puede adaptarse a su entorno. En particular, el proceso de gobernanza de Substrate permite cambios profundos en la cadena con coordinación mínima entre los distintos operadores de nodos.

recompensas de bloque

Quantus Network emplea un modelo de tokenómica sencillo que imita el de Bitcoin. Hay un suministro máximo de **21.000.000 monedas** y una heurística simple determina la recompensa por bloque:

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

Esta heurística forma una curva exponencial suavemente decreciente a medida que la block_reward contribuye al current_supply, lo que reduce la block_reward calculada en el siguiente bloque. Las quemas por comisiones u otras reducen el current_supply y pasan a formar parte del presupuesto de

recompensas de bloque. La constante se elige para que, sin ninguna quema, el 99% de las monedas se emita en unos 30 años.

asignación a inversores

Quantus Network se construyó con la ayuda de inversores que asumieron gran riesgo al financiarlo. Los inversores privados están sujetos a un calendario de adquisición de 4 años, como el equipo. Los inversores de la venta pública tendrán liquidez total el primer día. Los fondos recaudados en la venta pública se emparejarán con tokens y se usarán para liquidez (DEX, CEX y market makers). Estas asignaciones a inversores junto con la liquidez serán el único «pre-minado». El resto de tokens deberá minarse hasta existir.

Si se vende menos del máximo del 10% durante la venta pública, habrá una reducción proporcional de los tokens de liquidez y el resto se emitirá a mineros mediante recompensas de bloque.

asignación a la compañía

Para compensar al equipo por asumir el riesgo de construir tecnología nueva sin garantía de éxito, una parte de la recompensa de bloque se envía a la compañía durante unos cuatro años. Esto supone un calendario de adquisición de facto de unos **15% del suministro total** para la compañía.

Tras ese punto, la parte de la compañía en las recompensas de bloque puede apagarse, ajustarse o redirigirse según el voto de los titulares de tokens.

comisiones de transacción

TIPO DE TRANSACCIÓN	ESTRUCTURA DE COMISIÓN	DESTINO
Estándar	Comisión fija	Mineros
Reversible (alta seguridad)	1% sobre volumen	Quemada
Agregada ZK	0,1% sobre volumen	50% minero / 50% quemada

actualizaciones sin bifurcación

Quantus Network admite actualizaciones «sin bifurcación» mediante las actualizaciones de runtime de Substrate, permitiendo que la lógica central de la blockchain (el «runtime») evolucione sin hard forks que perturben la red o dividan la comunidad. Se logra mediante referendos de gobernanza en cadena, donde las propuestas aprobadas activan un intercambio de runtime — sustituyendo esencialmente el blob de código WASM existente por uno nuevo en un solo bloque, asegurando continuidad de estado y operaciones. Esta vía minimiza tiempos de inactividad y riesgos, empoderando a la comunidad para refinar el protocolo de forma iterativa a medida que el uso real revela mejoras.

A medida que la comunidad gana confianza en el sistema, el poder de cambiar el runtime se reducirá de forma significativa para limitar

la superficie de ataque si un actor malicioso obtiene el control del proceso de actualización.

sistema de gobernanza

Quantus Network hereda su marco de gobernanza del sistema OpenGov de Polkadot vía Substrate. Los titulares de tokens participan mediante **voto con convicción**, bloqueando sus activos durante periodos variables para amplificar el peso del voto. La amplificación puede ir de 1x (sin bloqueo) a 6x (bloqueo máximo). Este diseño fomenta la alineación a largo plazo vinculando influencia al compromiso.

Las propuestas se categorizan en múltiples pistas de votación llamadas «origins». Cada origin tiene parámetros a medida como umbrales de aprobación (p. ej., supermayoría para cambios de alto impacto), depósitos mínimos contra spam, periodos de preparación/ejecución y plazos de decisión para evitar bloqueos. Este diseño multipista permite procesar en paralelo referendos diversos, desde gastos rutinarios del tesoro hasta actualizaciones críticas de runtime.

El **Technical Collective** es un grupo curado de expertos técnicos que actúa como órgano especializado para proponer, revisar o incluir en lista blanca asuntos técnicos urgentes, acelerándolos por una pista dedicada manteniendo la supervisión comunitaria.

Quantus adopta este sistema sin modificaciones pero comienza con una configuración minimalista para evitar complejidad en las primeras etapas. Inicialmente, solo está activa la pista del Technical Collective, usada para decisiones vinculantes de alto privilegio como actualizaciones de protocolo o ajustes de parámetros.

Más adelante, Quantus puede añadir una pista de voto comunitario no vinculante para sondear el sentimiento sobre temas no exigibles, como sugerencias de funciones o encuestas del ecosistema. Este sistema se volverá vinculante cuando la compañía entregue la red al DAO. Este enfoque por fases permite que la red evolucione de forma orgánica mediante futuros votos de gobernanza sin cargar a los usuarios con complejidad innecesaria al principio.

07

hoja de ruta

La hoja de ruta actual hasta 2026, sujeta a cambios.

heisenberg inception Diciembre 2024	Financiación asegurada, Substrate elegido.
resonance alpha Julio 2025	Testnet pública, firmas Dilithium, transacciones reversibles.
schrödinger beta Octubre 2025	Funciones completas, listo para auditoría.
dirac beta Noviembre 2025	PoW cambiado a Poseidon2, auditorías abordadas.
planck beta Enero 2026	Cuentas de alta seguridad, multisig, monedero hardware, integración ZK.
bell mainnet Q2 2026	Lanzamiento de mainnet.
fermi upgrade Q4 2026	Infraestructura de agregación de pruebas ZK.

08

riesgos

Construir Quantus Network conlleva riesgos inherentes.

problemas de implementación

Defectos en la lógica del software pueden causar fallos graves incluso en los sistemas mejor diseñados.

problemas de selección de algoritmos del nist

Defectos o puertas traseras potenciales en estándares post-cuánticos seleccionados (p. ej., ML-DSA, ML-KEM) que podrían surgir tras la estandarización. En el peor caso, tales defectos permitirían a un atacante falsificar firmas derivando la clave privada de la pública, lo que representaría un modo de fallo catastrófico de la cadena. Si tales defectos se hicieran públicos, Quantus Network podría actualizarse a un nuevo algoritmo, pero si se explotan de forma escasa quizá nunca se descubran.

plazos de la computación cuántica

Los avances cuánticos podrían llegar mucho más tarde de lo previsto, retrasando la necesidad de PQC; a la inversa, un desarrollo secreto (p. ej. por gobiernos) podría generar amenazas repentinas si la comunidad blockchain no actualiza con rapidez.

otras consideraciones

Barreras generales de adopción, incertidumbre regulatoria en finanzas/blockchain y la volatilidad inherente de los ecosistemas cripto.

09

referencias y lecturas adicionales

[1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eight Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[3] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[4] National Institute of Standards and Technology. (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML- DSA)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[6] Häner, T., Jaques, S., Naehrig, M., Roetteler, M., & Soeken, M. (2020). Improved quantum circuits for elliptic curve discrete logarithms. *arXiv:2002.12480*. https://arxiv.org/abs/2002.12480

[7] Gidney, C., & Ekerå, M. (2021). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. *arXiv:1905.09749*. https://arxiv.org/abs/1905.09749

[8] Aggarwal, D., et al. (2021). Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies. *ePrint IACR*. https://eprint.iacr.org/2021/967.pdf

[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. *arXiv:1706.06752*. https://arxiv.org/abs/1706.06752

[10] Open Quantum Safe Project. (n.d.). ML-DSA | Open Quantum Safe. Retrieved January 29, 2026, from https://openquantumsafe.org/liboqs/algorithms/sig/ml-dsa.html