KELYRIUM

LIBRO BLANCO DE LA RED

Arquitectura técnica y especificación económica · V1.3

COFUNDADORES

Abraham Gómez
Gerardo Gómez

23 de octubre de 2026

Kelyrium.org • Kelyrium.com

VERSION 1.3 | TECHNICAL DESIGN DRAFT

Una cadena. Veinticinco activos nativos. Participación abierta.

Borrador técnico actualizado | 23 de octubre de 2026

Kelyrium.org • Kelyrium.com

Resumen

Kelyrium es un proyecto de red independiente de capa 1, de código abierto y basada en prueba de trabajo (PoW), desarrollada mediante una implementación original en Rust; no es una bifurcación de Bitcoin Core con otro nombre. Un único historial de consenso admite KELY, la moneda principal de la red, y 24 activos nativos Bitcoin World, cada uno con su propio límite de emisión. Según el diseño de recompensas revisado, cada bloque válido minado emite una asignación determinista para los 25 activos nativos.

El protocolo busca combinar minería de CPU y GPU sin permisos, billeteras bajo control del usuario, liquidación directa entre activos, contratos inteligentes EVM deterministas, tokens fungibles creados por terceros, NFT y funciones opcionales de privacidad. Los servicios semilla facilitan el descubrimiento de pares, pero carecen de privilegios sobre los saldos y el consenso.

Este documento presenta la arquitectura actualmente prevista. Las funciones descritas como planificadas o candidatas no se consideran implementadas ni auditadas. Los parámetros definitivos y la seguridad de la red principal deben acreditarse mediante pruebas reproducibles y revisiones independientes.

1. Alcance y estado de las especificaciones

Esta publicación V1.3 define el diseño inicial de la red de 25 activos, sus parámetros monetarios, requisitos de seguridad y pruebas de ingeniería. Es una propuesta de capa 1 independiente; las funciones planificadas no implican implementación ni auditoría completadas.

El intervalo de 30 segundos y la recalibración de recompensas y reducciones a la mitad son la dirección actual de diseño, no resultados demostrados en producción. Se propone una madurez de coinbase de 120 bloques, aún sin ratificar. Los implementadores no deben inventar sin revisión parámetros de consenso como formatos binarios, coeficientes de comisiones, algoritmos de hash o sistemas de pruebas criptográficas.

Los 25 activos nativos definidos por el protocolo no deben confundirse con la cantidad potencialmente ilimitada de tokens creados mediante contratos. Estos últimos siguen sus propias reglas y no pueden modificar el registro monetario nativo.

- Consenso: L1 PoW independiente; doble vía CPU/GPU bajo evaluación
- Bloques: objetivo de 30 segundos, pendiente de pruebas globales
- Activos nativos: 25 en total, KELY y 24 Bitcoin World
- Precisión: 12 decimales por activo, enteros u128 comprobados
- Máximo KELY: 21.000.000, incluida génesis de 630.000
- Subvención inicial: 2,425 KELY por bloque de 30 segundos, propuesta
- Reducción a la mitad: 4.200.000 bloques (aprox. cuatro años)
- Madurez coinbase: 120 bloques propuestos, sin ratificar

- Presupuesto inicial de bloque: 192.000 bytes, por revisar
- Contratos: EVM determinista, ERC-20/721/1155 planificados
- Privacidad: billetera respetuosa, blindaje futuro opcional y auditado
- Gas: KELY como base, patrocinio de comisiones propuesto
- Actualizaciones: KIP públicos, activación versionada y sin administrador
- Mainnet: testnet pública ≥90 días, últimos ≥30 estables y revisión

2. Una cadena y validación independiente

Kelyrium dispone de un solo libro mayor entre pares y un único historial global de bloques, no de 25 cadenas minadas por separado. Cada nodo completo verifica de manera independiente la prueba de trabajo, la conservación de cada activo, las autorizaciones de gasto, la emisión coinbase, las transiciones contractuales y los compromisos de los bloques. Ninguna semilla DNS, nodo inicial, pool, servidor de billetera o explorador puede reescribir el libro mayor con privilegios especiales.

El intervalo objetivo es de aproximadamente 30 segundos. El presupuesto serializado candidato del diseño original es de 192.000 bytes por bloque, incluidas firmas y pruebas. La configuración definitiva dependerá de las mediciones de propagación global, bloques competidores, reorganizaciones, dificultades de CPU/GPU y coste de los nodos. Además de los bytes, deben limitarse el gas de cómputo y el crecimiento del estado permanente.

El descubrimiento de pares utilizará varias semillas DNS independientes, pares conocidos y nodos especificados por el usuario. Conforme aumente la diversidad geográfica de nodos completos y mineros independientes, debe disminuir la dependencia de servidores operados por el propio proyecto.

3. Registro génesis V1.3 y política monetaria

La tabla define el registro inicial completo. Cada activo tiene un país o región, una moneda de referencia, un suministro máximo y una recompensa propuesta para la primera época. Los 25 activos pertenecen a una sola blockchain. Sus nombres no implican paridad, respaldo ni convertibilidad en moneda fiduciaria.

País / Región	Moneda	Activo	Suministro máximo	Recompensa inicial
Global / Red Kelyrium	Kelyrium	KELY	21,000,000	2.425
Estados Unidos	US Dollar	BTC-USD	210,000,000	25
Eurozona	Euro	BTC-EURO	189,000,000	22.5
Japón	Japanese Yen	BTC-YEN	2,100,000,000	250
China	Chinese Yuan	BTC-YUAN	630,000,000	75
Reino Unido	British Pound	BTC-POUND	105,000,000	12.5
Vietnam	Vietnamese Đồng	BTC-VND	21,000,000,000	2500
México	Mexican Peso	BTC-PESOM	420,000,000	50
Tailandia	Thai Baht	BTC-BAHT	840,000,000	100
India	Indian Rupee	BTC-RUPEE	1,050,000,000	125
Corea del Sur	South Korean Won	BTC-WON	4,200,000,000	500
Rusia	Russian Ruble	BTC-RUBLE	1,260,000,000	150

País / Región	Moneda	Activo	Suministro máximo	Recompensa inicial
Suiza	Swiss Franc	BTC-FRANC	84,000,000	10
Turquía	Turkish Lira	BTC-LIRA	1,680,000,000	200
Brasil	Brazilian Real	BTC-REAL	315,000,000	37.5
Arabia Saudita	Saudi Riyal	BTC-RIYAL	168,000,000	20
Emiratos Árabes Unidos	UAE Dirham	BTC-DIRHAM	147,000,000	17.5
Taiwán	New Taiwan Dollar	BTC-TWD	1,344,000,000	160
Polonia	Polish Złoty	BTC-ZLOTY	378,000,000	45
Hong Kong	Hong Kong Dollar	BTC-HKD	336,000,000	40
Indonesia	Indonesian Rupiah	BTC-RUPIAH	10,500,000,000	1250
Filipinas	Philippine Peso	BTC-PESOP	735,000,000	87.5
Canadá	Canadian Dollar	BTC-CAD	231,000,000	27.5
Australia	Australian Dollar	BTC-AUD	294,000,000	35
Singapur	Singapore Dollar	BTC-SGD	126,000,000	15

El intervalo objetivo de 30 segundos, la reducción cada 4.200.000 bloques y la recompensa simultánea para los 25 activos son parámetros de diseño. Antes de mainnet deben verificarse los calendarios exactos de emisión con aritmética entera.

4. Emisión, génesis y recompensas mineras

Cada bloque válido incluye recompensas deterministas para KELY y los 24 activos regionales. Mineros y pools no pueden omitir ni sustituir recompensas.

El intervalo objetivo de 30 segundos, la reducción cada 4.200.000 bloques y la recompensa simultánea para los 25 activos son parámetros de diseño. Antes de mainnet deben verificarse los calendarios exactos de emisión con aritmética entera.

La asignación génesis de KELY sigue siendo de 630.000 monedas (el 3 % de los 21 millones): 210.000 para el fundador y 420.000 para operaciones, repartidas en 75 salidas sujetas a seguimiento del vesting. Para el fundador se prevén 21.000 elegibles inicialmente, 31.500 en el mes 12 y 36 entregas de 4.375 entre los meses 13 y 48. Para operaciones se prevén 63.000 iniciales y 36 cuotas redondeadas exactamente a enteros que suman 357.000 durante los meses 1 a 36. Todas están dentro del límite de emisión y sujetas a las condiciones temporales y de firma previstas.

Se planifican saldos génesis nulos para los 24 activos secundarios. La nueva cesta de recompensas deberá comprobarse frente a cada suministro máximo inmutable. Restos de unidades básicas, compromisos coinbase, restricciones de desbloqueo y reorganizaciones profundas requieren reglas exactas. La madurez de 120 bloques (unos 60 minutos a 30 segundos) sigue siendo una propuesta.

5. Prueba de trabajo y pools de minería

Se conservan dos modalidades PoW —CPU y GPU— que compiten por extender una única cadena global, cada una con su propia contabilidad de dificultad y una comparación formal de trabajo acumulado. La evaluación original consideró yespower para CPU y KawPow para GPU, con Verthash como alternativa. Ninguna puede garantizar resistencia absoluta a ASIC; la selección definitiva queda sujeta a pruebas y revisión de seguridad.

Los usuarios podrán minar individualmente o seleccionar pools independientes dentro de la billetera. El directorio indicará comisiones, región, latencia, operador, dificultad de participaciones, modalidad de pago, madurez, umbral y rendimiento. Los usuarios de poca potencia aportan participaciones válidas sin necesidad de encontrar solos un bloque. Los pools podrán distribuir la cesta de 25 activos; cualquier conversión voluntaria a un único activo requerirá liquidez verificable y cotizaciones claras.

La contabilidad de pools debe resistir participaciones manipuladas, ocultación de bloques, trabajo obsoleto, reorganizaciones, recompensas inmaduras y concentración de control. Los pools sin permisos de tipo P2Pool son materia de investigación. La seguridad exige medir no solo la potencia nominal, sino la diversidad de nodos, mineros y pools.

6. Libro mayor nativo y autocustodia

El libro mayor básico es un modelo UTXO multiactivo y versionado, con conservación independiente de saldos por activo. Los pagos corrientes autentican la propiedad de las entradas y crean salidas explícitas. Entre las condiciones candidatas de gasto se encuentran firmas de una sola clave, umbrales, bloqueos, caducidad y criptografía Schnorr revisada. Las firmas deben vincular el dominio de la cadena, el identificador del activo, el importe, el destinatario y el contexto de la transacción.

El consenso debe rechazar gastos dobles, entradas duplicadas, recompensas coinbase ilegales, codificaciones no canónicas y desbordamientos aritméticos. Las reorganizaciones revertirán de modo atómico UTXO, emisiones acumuladas y estados EVM antes de aplicar el historial válido.

Las billeteras podrán gestionar varias identidades y frases de recuperación independientes, generar direcciones nuevas y administrar los 25 activos en una sola aplicación. Son prioritarios el almacenamiento cifrado, las copias de seguridad, las vistas previas de firma y el control de monedas. Crear múltiples direcciones no garantiza el anonimato en cadena.

7. Comisiones bajas, precios de recursos y patrocinio de gas

KELY es el activo principal para pagar los costes de red. El objetivo son transferencias muy económicas, pero no recursos ilimitados a coste cero. La política de comisiones debe equilibrar el acceso de usuarios legítimos con el coste económico de los ataques sostenidos de congestión.

Las transferencias simples evitarán el cómputo EVM innecesario. La ejecución de contratos, escritura de estado persistente, verificación de pruebas, creación de UTXO y uso de datos pagarán conforme a los recursos utilizados, con ajustes por demanda. Se medirán y limitarán independientemente bytes, CPU, memoria, almacenamiento y crecimiento del estado.

Para billeteras sin KELY se estudia permitir que un patrocinador autorizado pague las comisiones en KELY y reciba reembolso en otro activo compatible. Se requieren cuotas autenticadas, caducidad, liquidación atómica, firmas, límites de velocidad y precios claros. El reconocimiento directo de gas en activos distintos de KELY por el consenso es una decisión separada todavía no aprobada.

8. Contratos inteligentes, tokens y NFT

Kelyrium prevé un entorno de ejecución EVM compatible y determinista en la misma capa 1. Solidity y sus herramientas solo podrán considerarse compatibles cuando se implementen realmente RPC, compromisos de estado, recibos, medición de gas y ejecución correcta ante reorganizaciones. El despliegue de tokens fungibles ERC-20 es un objetivo explícito para el lanzamiento; los estándares ERC-721 y ERC-1155 cubrirán NFT y coleccionables.

Los tokens de contratos no se añaden a la lista de 25 activos nativos. Sus cantidades, facultades de emisión y quema, decimales y permisos de actualización dependerán de contratos públicos. Podrán coexistir contratos inmutables y proxies actualizables con autoridades divulgadas. La billetera y el explorador advertirán sobre administradores, aprobaciones peligrosas y código no verificado.

La frontera contable entre UTXO y EVM exige conversiones enteras exactas entre 12 decimales nativos y unidades EVM, prepago y reembolsos de gas, liquidación atómica, límites de almacenamiento y reversión determinista. Ningún contrato puede generar KELY o Bitcoin World fuera de la emisión PoW. El asistente de creación de tokens y el mercado NFT son funciones de aplicación y no garantizan seguridad, precio ni liquidez.

9. Intercambio nativo, dinero fiduciario e interoperabilidad

El intercambio descentralizado previsto emplea órdenes P2P firmadas y bajo autocustodia, con liquidación atómica entre activos nativos, cancelación, vencimiento, reserva segura de entradas y protección contra repetición. Como los 25 activos comparten una cadena, intercambiarlos no exige un puente externo. Cuando existan liquidez suficiente, límites adecuados y ejecución segura, podrán usarse rutas a través de KELY.

Un usuario nuevo puede crear una dirección y recibir fondos sin minar. También puede adquirir activos de otros titulares o comprarlos en mercados externos donde estén listados. La compra mediante dinero fiduciario requiere un proveedor real de pagos, oferta y liquidez auténticas y medidas de identidad o cumplimiento legal cuando correspondan. Ningún nombre regional convierte automáticamente moneda nacional en activos recién creados.

La billetera podrá incorporar con el tiempo adaptadores modulares para Bitcoin, redes EVM y Solana. Mostrar o firmar transacciones de otras cadenas no equivale a trasladar valor entre ellas. Los puentes requieren modelos de confianza específicos y auditorías independientes, y no son funciones implícitas del lanzamiento inicial.

10. Verificabilidad pública y privacidad opcional por fases

La estrategia de privacidad de Kelyrium se basa en una billetera cuidadosa con la privacidad desde el inicio, con futuros pagos blindados opcionales semejantes a los de Zcash y una modalidad pública o transparente explícita. Las protecciones iniciales incluyen custodia local de claves, respaldos cifrados, control UTXO, rotación de direcciones, telemetría mínima y transportes opcionales como Tor o I2P. Por sí solas no ocultan criptográficamente los importes ni las contrapartes visibles.

El blindaje verdadero deberá proteger detalles apropiados sin impedir que los nodos validen la conservación y límites de emisión de cada activo. Se investigan compromisos criptográficos, nullifiers, pruebas de saldo de conocimiento cero, claves de visualización o divulgación, medición del coste de pruebas y recuperación segura. El sistema de prueba, las operaciones admitidas, el escaneo de billetera y la fecha de integración siguen sin decidirse y requieren auditoría especializada.

La actividad EVM corriente, intercambios transparentes, salidas de recompensa y movimientos entre dominios blindados y transparentes pueden revelar metadatos. La billetera deberá explicar estas limitaciones. El explorador público mostrará datos de consenso, emisión por activo, compromisos de transacciones y contratos visibles, sin afirmar que puede revelar información correctamente protegida. No se prevé un mezclador custodial ni una clave privilegiada para congelar arbitrariamente fondos.

11. Seguridad, antispam y resiliencia operativa

Defensas de consenso: formatos canónicos y acotados para bloques y transacciones; invariantes de cada activo; aritmética comprobada; separación de dominios de firmas y pruebas; límites de ejecución y almacenamiento; gas determinista; madurez coinbase y reversión completa durante reorganizaciones.

Defensas económicas: comisiones no nulas ponderadas por recursos, precios según demanda, costes de creación de UTXO, políticas antidust y cargos por estado persistente. Deben modelarse ataques con millones de transferencias económicas, acumulación masiva de UTXO, crecimiento forzado de contratos y manipulación de congestión. Las normas locales del mempool y de retransmisión no deben confundirse con las reglas de validez consensuadas.

Defensas P2P y RPC: límites independientes de bytes, CPU, memoria, conexiones, solicitudes pendientes, profundidad de colas, tamaño de mensajes y consultas históricas costosas. El tráfico malformado se descartará antes de gastar recursos en criptografía. Se investigará la diversidad de pares y la resistencia a ataques eclipse y Sybil, evitando expulsar sistemáticamente a usuarios legítimos de redes compartidas.

Defensas de aplicación: firmas seguras y avisos de phishing; simulación de interacciones con contratos; divulgación de administradores de actualización; cuotas y firmas de patrocinadores; verificación de participaciones mineras; aislamiento de adaptadores externos y límites al coste de pruebas de conocimiento cero. Ninguna medida elimina todos los riesgos futuros: hacen falta fuzzing, simulaciones adversariales, compilaciones reproducibles, auditorías independientes, divulgación responsable y respuesta ante incidentes.

12. Actualizaciones, compatibilidad y gobernanza

Los componentes de consenso y red tendrán versiones explícitas. Los cambios se tramitarán mediante Kelyrium Improvement Proposals (KIP) públicos, especificaciones de referencia, vectores de prueba, revisión independiente, activación en testnet y plazos de publicación anunciados. La negociación de capacidades entre pares puede acordar funciones de red compatibles, pero no distintas reglas activas de validez de consenso.

Billeteras, indexadores, clientes de minería y adaptadores de red podrán actualizarse por separado cuando se mantenga la compatibilidad. Los desarrolladores de contratos elegirán entre implementaciones inmutables y proxies transparentemente actualizables, preferiblemente con multifirma y timelocks. Los administradores de billeteras o contratos no podrán alterar los límites nativos ni confiscar fondos arbitrariamente.

Toda actualización de consenso deberá describir compatibilidad, altura de activación, posible bifurcación, recuperación y procedimientos de publicación multipartitos. Los servidores semilla del proyecto no tienen privilegios de administración de la red.

13. Implementación y criterios de lanzamiento

Fase A — especificación y contabilidad: reconciliar el programa económico original, el código fuente y los 12 decimales aprobados; definir identificadores, génesis, vesting, vectores de recompensas, formatos de bloques y transacciones, unidades de comisiones y pruebas deterministas comunes a múltiples lenguajes.

Fase B — prototipos de consenso: medir minería CPU/GPU y recuperación de dificultad, contabilidad UTXO multiactivo, ejecución EVM determinista, serialización de las 25 recompensas, invariantes de suministro, reorganizaciones y rendimiento de nodos a intervalos alternativos de 30 y 60 segundos.

Fase C — software para usuarios: entregar billeteras Windows/Linux, nodos CLI sin interfaz en Ubuntu, integración con pools independientes, explorador verificable, intercambio por órdenes firmadas, transferencias nativas, despliegue de tokens y NFT. El blindaje avanzado, proveedores fiduciarios y puentes externos pueden necesitar fases separadas.

Fase D — testnet pública y revisión independiente: publicar código reproducible, operar al menos 90 días de testnet pública, exigir estabilidad durante los 30 días finales, probar ataques y encargar revisión independiente del consenso, criptografía, emisión, comportamiento EVM y correcciones. Solo lanzar la red principal tras cumplir criterios documentados; no se garantiza fecha ni precio alguno.

14. Limitaciones y agenda de investigación

Los mayores riesgos técnicos siguen siendo la comparación de trabajo acumulado entre dos algoritmos, el crecimiento de UTXO por 25 recompensas, la integración exacta UTXO/EVM, la economía del gas y estado permanente, los sistemas de blindaje opcionales, la recuperación de billeteras, la confianza en pools y la interoperabilidad externa. Los bloques de 30 segundos y las comisiones bajas implican compromisos medibles, no escalabilidad automática.

El experimento inicial desechable en Rust validó aritmética de emisión y vesting con 11 pruebas multiplataforma; no estableció criptografía terminada, red segura, conformidad EVM, transferencias blindadas, rentabilidad minera, billetera auditada ni preparación para mainnet. Toda afirmación futura debe basarse en resultados de implementación verificables.

Referencias e historial documental

Kelyrium Network, White Paper 1.0 Draft (15 de septiembre de 2026); Kelyrium Consolidated Architecture & Design Decision Record V1.2 (23 de octubre de 2026); Kelyrium Master Implementation Prompt for Claude/Astra/Codex V1.2 (23 de octubre de 2026).

Antecedentes técnicos públicos: Bitcoin: A Peer-to-Peer Electronic Cash System; documentación de gas y EVM de Ethereum; especificaciones ERC-20, ERC-721 y ERC-1155; investigaciones sobre minería P2P y seguridad de billeteras. Son referencias de diseño, no declaraciones de afiliación.

Derechos de autor y autoría

Copyright © 2026 Abraham Gómez y Gerardo Gómez. Todos los derechos reservados.
Libro Blanco de Kelyrium · Borrador técnico V1.3 · 23 de octubre de 2026.

Este documento se facilita para revisión y debate técnico. La autorización para citarlo o compartirlo con atribución no concede una licencia sobre marcas de Kelyrium, ilustraciones u otros materiales protegidos por separado. Los componentes de software de código abierto, cuando se publiquen, estarán sujetos a sus respectivas licencias oficiales.