

cosigo — Libro blanco (español)

Modelo de ficha respaldada por plata física • Contrato principal y satélites con Guardian

Resumen ejecutivo

cosigo es un sistema de fichas digitales donde **1 cosigo = 1 mg de plata física (Ag)**. El contrato principal (cosigo_) registra depósitos de plata, define la acuñación contra “espacio disponible” y permite rescates físicos bajo políticas de mercado; los **contratos satélite** heredan la economía base, añaden límites y funciones locales (ciudades/puntos de custodia) y están sujetos a límites globales definidos por un **Guardian**. El objetivo es ofrecer una capa de confianza y trazabilidad en la relación entre el activo físico y su representación digital, con controles operativos y de seguridad que priorizan el cumplimiento del “ancla de valor” y la protección del usuario.

Principios de diseño

- Valor, no precio: la ficha expresa miligramos de plata, evitando la volatilidad de monedas fiat.
- No inflacionario: la acuñación solo procede contra depósitos físicos registrados y verificados.
- Rescate físico transparente: solicitudes en cadena con seguimiento, límites diarios y políticas de mercado.
- Gobernanza operativa mínima: roles claros (propietario, custodio, Guardian) y timelocks para cambios sensibles.

Arquitectura técnica (alto nivel)

La arquitectura consta de tres capas: (1) Contrato principal cosigo_: custodia lógica de depósitos (gramos→mg), cálculo de espacio disponible, rescate físico y parámetros de mercado; (2) CosigoSatellite: instancias locales con límites y tasas propios, sujetos a límites globales; (3) Guardian: registro/aprobación de satélites, topes máximos de tarifas y primas, y señales de mercado (‘mercado abierto/cerrado’).

Economía del token (tokenomics)

- Unidad: 1 cosigo = 1 mg de plata (18 decimales).
- Depósitos: registro en cadena; cada entrada incluye hash documental verificable y sello de tiempo.
- Acuñación: solo contra espacio disponible (mg depositados – tokens en circulación/pedidos).
- Rescate: quema de tokens (+ tarifa) y cumplimiento físico por custodio.
- Tarifas: mantenimiento en transferencias, tarifa de rescate y prima sobre spot.
- Guardian skim: recorte global configurable por Guardian durante transferencias.

Parámetros operativos clave

- spotMicroCentsPerMg y minFloorMicroCentsPerMg: controlan el ‘piso’ mínimo para rescates.
- maintenanceFeeBps, redemptionFeeBps, premiumBps: tasas locales con topes locales y globales.
- dailyCapPerAddrMg1e18 y dailyCapGlobalMg1e18: límites diarios de rescate por cuenta y globales.
- minRedemptionMg1e18: tamaño mínimo de rescate.
- paramTimelockSeconds: retardo obligatorio para cambios sensibles.

Flujos principales

- Depósito y registro: el custodio registra un depósito con docHash y cantidad en gramos.
- Acuñación contra espacio disponible: minters autorizados acuñan solo si no se excede el headroom.

- Transferencias: aplican tarifa de mantenimiento y recorte global del Guardian antes de acreditar.
- Rescate físico: se queman tokens (+ tarifa) y se crea un ID para cumplimiento físico. Cancelar devuelve tokens, la tarifa permanece quemada.

Seguridad y gobierno

- Pausas y emergencia: detener operaciones en casos críticos.
- Listas negras: bloqueo de direcciones con motivo.
- Anti-bot: límites de gas, retardos, solo EOA.
- Guardian: topes máximos, registro de satélites, señales de mercado.
- Timelock de parámetros: cambios en cola hasta expirar el retardo.
- Rescate de tokens ajenos: mover ERC-20 enviados por error (no el propio).

Contratos satélite (CosigoSatellite)

Cada satélite se despliega con un slug de ciudad ('cosigo_'). Incluyen límites locales de tarifas, sumideros locales, mínimos de rescate, contadores diarios y listas negras. Separan mg pendientes y mg cumplidos para evitar 'resurrección de espacio'.

Límites locales y globales

- Local: MAX_MAINTENANCE_FEE_BPS, MAX_REDEMPTION_FEE_BPS, MAX_PREMIUM_BPS.
- Global: definidos por Guardian.
- En transferencias: guardianChecks valida condiciones globales antes de asentarlas.

Roles locales

- Admin: gobierna parámetros y timelocks.
- Custodio: registra depósitos y cumple/cancela rescates.
- Minter: acuña contra espacio disponible.
- Pauser: pausa/reanuda operaciones.

Interfaz pública principal

- Consultas: effectiveSupply, headroomMg1e18, depositsLength, parámetros de mercado.
- Control: setMaintenanceFeeBps, setRedemptionFeeBps, setPremiumBps, setSpotMicroCentsPerMg.
- Flujo de rescate: redeemPhysicalSilver, fulfillRedemption, cancelRedemption.
- Eventos: DepositRegistered, MaintenanceFeeSet, RedemptionRequested/Fulfilled/Cancelled, GuardianFeeSkim, etc.

Guía de despliegue de satélite

- Elegir slug (min 4, max 32).
- Inicializar Guardian y aceptar topes globales.
- Configurar sumideros locales (tarifa/quema).
- Asignar roles: admin, custodio, minter.
- Establecer parámetros: tarifas, primas, mínimos y límites diarios.
- Publicar procedimiento de rescate (plazos, logística, costos).

Anexo técnico

El contrato principal y los satélites exponen constructores, errores, eventos y funciones de gestión de mercado, depósitos y rescates. Se recomienda revisar el código fuente para detalles exactos. Este anexo resume funciones sin tablas para evitar solapamiento.

Aviso

Documento informativo. No constituye asesoría financiera ni oferta de valores. Las implementaciones deben auditarse y configurarse conforme a leyes locales y prácticas de seguridad.