

Billeteras Deterministas por Licencia (BDL)

Índice formal — Marco metodológico y especificación académica (alcance exclusivo: billetera de licencias)

Diseñado por LAEV Blockchain 

Autor: Larry Alexander Elizondo Villalobos

0. Declaración de alcance y propósito

- 0.1 Objetivo epistemológico y técnico del documento
- 0.2 Alcance delimitado: definición exhaustiva de la Billetera Determinista por Licencia (BDL)
- 0.3 Exclusiones explícitas y no-objetos de estudio
- 0.4 Audiencia especializada: arquitectura de sistemas, criptografía aplicada, seguridad, producto y auditoría
- 0.5 Convenciones formales, notación criptográfica y criterios de lectura

1. Fundamentos byLAEV: filosofía profesional y metodología aplicada a BDL

- 1.1 Principio de integridad pública verificable: documentación completa, reproducibilidad y auditabilidad
- 1.2 Principio de trazabilidad mínima suficiente: evidencia técnica sin exposición de material sensible
- 1.3 Principio de no-simulacro técnico: exclusión de afirmaciones no demostrables o no enforceables
- 1.4 Principio de responsabilidad estructural: separación estricta entre diseño, operación y verificación independiente
- 1.5 Principio de presencia metodológica: registro continuo de decisiones, cambios y versiones (metodología byLAEV)
- 1.6 Principio de diseño sistémico-industrial: coherencia entre experiencia de usuario y restricciones criptográficas reales
- 1.7 Criterio de verdad operativa: distinción formal entre normas de uso, políticas y restricciones técnicas

2. Definiciones formales y glosario técnico

- 2.1 BDL (Billetera Determinista por Licencia): definición normativa
- 2.2 Licencia: identidad criptográfica, cupo operativo, política y régimen de vigencia
- 2.3 Dispositivo: identidad criptográfica verificable (DeviceID) y evidencias opcionales de hardware (attestation)
- 2.4 Registro de licencias: ledger basado en event-sourcing y verificación determinística
- 2.5 Tipología de eventos: GENESIS, ACTIVATE, DEACTIVATE, ROTATE, ALERT
- 2.6 Anclaje en Bitcoin: compromisos criptográficos, Merkle root y pruebas de inclusión temporal
- 2.7 Sistema de alertas: métricas, severidad acumulada y códigos de razón
- 2.8 Gobernanza: llaves, quórum, procesos de revocación y re-emisión
- 2.9 Enforceability: condiciones técnicas mínimas para garantizar "N dispositivos"

3. Planteamiento formal del problema

- 3.1 Limitación estructural: copiabilidad inherente de seeds y claves privadas
- 3.2 Objetivo funcional: correspondencia controlada entre una licencia y un conjunto finito de dispositivos autorizados
- 3.3 Objetivo operacional: detección, registro y trazabilidad de intentos fuera de política
- 3.4 Objetivo económico y de producto: emisión, entrega y administración de licencias de uso
- 3.5 Objetivo de auditoría: generación de evidencia pública verificable sin custodia de secretos

4. Modelo de amenazas (Threat Model)

- 4.1 Amenazas primarias: clonación de seed, duplicación de instalaciones, ataques de replay y suplantación
- 4.2 Amenazas secundarias: exfiltración de DeviceID, manipulación de eventos, indexadores maliciosos
- 4.3 Amenazas sistémicas: coerción del usuario, pérdida de dispositivos, colusión entre actores
- 4.4 Supuestos explícitos del modelo de seguridad
- 4.5 Estrategias de mitigación clasificadas por severidad e impacto

5. Requisitos del sistema (System Requirements Specification)

- 5.1 Requisitos funcionales (FR): activación, control de cupo y operación bajo licencia
- 5.2 Requisitos no funcionales (NFR): disponibilidad, latencia, coste, escalabilidad y resiliencia
- 5.3 Requisitos de seguridad: autenticidad, integridad, no repudio y auditabilidad
- 5.4 Requisitos de privacidad: minimización de datos, seudonimización y consentimiento explícito
- 5.5 Requisitos de interoperabilidad: compatibilidad con billeteras HD y estándares existentes

6. Arquitectura de referencia del sistema BDL

- 6.1 Capas funcionales: cliente de billetera, registro de eventos, indexación distribuida y anclaje en Bitcoin
- 6.2 Identidades fundamentales: LicenseID y DeviceID
- 6.3 Flujos operativos: instalación, activación, operación, revocación y reemplazo
- 6.4 Estados formales de licencia: activa, suspendida, revocada y cupo agotado
- 6.5 Descentralización operativa: mecanismos de consenso del registro

7. Identidad de Licencia (LicenseID) y evento GENESIS

- 7.1 Construcción criptográfica de LicenseID: hashing, versionado y metadata
- 7.2 Evento GENESIS: definición inicial de cupo, política, llaves de gobernanza y parámetros
- 7.3 Representación de la licencia para emisión y entrega
- 7.4 Separación conceptual crítica: credencial de control vs. estado registrado
- 7.5 Régimen de vigencia: licencias perpetuas, temporales y mecanismos de expiración

8. Identidad de Dispositivo (DeviceID)

- 8.1 Generación local de pares de claves y no exportación recomendada
- 8.2 Construcción determinística de DeviceID

- 8.3 Attestation opcional: clasificación de niveles de confianza por plataforma
- 8.4 Riesgos de fingerprinting y estrategias de mitigación
- 8.5 Garantías de unicidad y análisis de colisiones

9. Registro descentralizado de licencias (Ledger por Event-Sourcing)

- 9.1 Modelo formal: eventos firmados y derivación determinística de estado
- 9.2 Reglas de validación y aceptación de eventos
- 9.3 Resolución de conflictos, ordenamiento y consistencia
- 9.4 Indexación múltiple y verificación independiente
- 9.5 Persistencia, replicación y disponibilidad del registro

10. Activación y control de cupo de dispositivos

- 10.1 Evento ACTIVATE: alta controlada de dispositivo bajo una licencia
- 10.2 Políticas de cupo: límites máximos, reservas y contingencias
- 10.3 Condiciones de enforceability: negación efectiva de operaciones fuera de política
- 10.4 Evento DEACTIVATE: baja voluntaria y baja por motivos de seguridad
- 10.5 Reemplazo de dispositivos (swap): procedimiento formal
- 10.6 Mecanismos de recuperación sin degradar el control de cupo

11. Operación de la billetera bajo régimen de licencia

- 11.1 Definición de operaciones críticas y precondiciones
- 11.2 Pruebas de autorización: verificación de DeviceID activo
- 11.3 Políticas de sesión, revalidación periódica y control de frecuencia
- 11.4 Compatibilidad HD: derivación de claves sin ruptura del modelo de licencias
- 11.5 Gestión de secretos locales, copias de seguridad y rotación

12. Sistema de alertas y puntuación de riesgo

- 12.1 Evento ALERT: definición formal, formatos y severidad
- 12.2 Modelos de puntuación: funciones de peso, ventanas temporales y umbrales
- 12.3 Respuestas automáticas basadas en política: suspensión y escalamiento
- 12.4 Evidencia técnica: trazabilidad de intentos no autorizados
- 12.5 Evaluación de alertas: análisis de falsos positivos y negativos

13. Anclaje criptográfico en la red Bitcoin

- 13.1 Compromisos periódicos: Merkle root de eventos y frecuencia óptima
- 13.2 Pruebas de inclusión y verificación externa independiente
- 13.3 Análisis de costes y estrategias de batching
- 13.4 Garantías de inmutabilidad y timestamp: alcance y limitaciones
- 13.5 Evidencia documental asociada exclusivamente a la billetera de licencias

14. Gobernanza y administración del ciclo de vida de licencias

- 14.1 Estructura de llaves de gobernanza: multisig, quórum y roles
- 14.2 Evento ROTATE: actualización de políticas y llaves
- 14.3 Evento REVOCATION: revocación definitiva y criterios objetivos
- 14.4 Re-emisión y migración controlada de licencias
- 14.5 Independencia del auditor y procesos de verificación externa

15. Privacidad, seguridad y cumplimiento normativo

- 15.1 Principio de minimización: límites estrictos al registro de datos
- 15.2 Seudonimización sistemática de LicenseID y DeviceID
- 15.3 Protección de metadata: riesgos y contramedidas
- 15.4 Controles técnicos: anti-replay, anti-forgery y anti-tamper
- 15.5 Preparación para auditorías sin custodia de información sensible

16. Implementación de referencia

- 16.1 Formatos de mensajes (JSON/CBOR), versionado y compatibilidad
- 16.2 Selección de librerías criptográficas y consideraciones de seguridad
- 16.3 Requisitos del cliente: móvil, escritorio y hardware especializado
- 16.4 Requisitos de indexadores: disponibilidad, verificación y caching
- 16.5 Estrategias de prueba: unitarias, integración y pruebas adversariales

17. Métricas y criterios de evaluación

- 17.1 Indicadores clave de licenciamiento: activaciones, revocaciones y reemplazos
- 17.2 Indicadores de seguridad: intentos rechazados, severidad acumulada y tiempos de respuesta
- 17.3 Indicadores de auditoría: verificaciones independientes y latencia de anclaje
- 17.4 Indicadores de experiencia: fricción operativa, recuperación y soporte
- 17.5 Plantilla estándar de reporte para partes interesadas

18. Conclusiones formales

- 18.1 Afirmaciones técnica y empíricamente garantizables
- 18.2 Afirmaciones explícitamente excluidas por no ser enforceables
- 18.3 Definición final de BDL como clase formal de billetera

Anexos

- A. Catálogo de códigos de razón (reason_code) para ALERT
- B. Diagrama formal de estados de LicenseID
- C. Plantillas de evidencia y auditoría técnica
- D. Vectores de ataque y matrices de mitigación
- E. Notas de interoperabilidad con estándares HD