Billeteras Deterministas por Licencia (BDL)

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

Diseñado por LAEV Blockchain 🦩
Autor: Lerry Alexander Elizondo Villalobos

---

0. Declaración de alcance y propósito

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

2. Definiciones formales y glosario técnico

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

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

10. Activación y control de cupo de dispositivos

11. Operación de la billetera bajo régimen de licencia

12. Sistema de alertas y puntuación de riesgo

13. Anclaje criptográfico en la red Bitcoin

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