Deterministic License-Based Wallets (DLBW)

Formal Index — Methodological and Academic Specification (exclusive scope: license-based wallet)

Designed by LAEV Blockchain 🦩
Author: Lerry Alexander Elizondo Villalobos

---

0. Scope and Purpose Statement

0.1 Epistemological and technical objective of the document
0.2 Delimited scope: exhaustive definition of the Deterministic License-Based Wallet (DLBW)
0.3 Explicit exclusions and non-subjects of study
0.4 Specialized audience: systems architecture, applied cryptography, security, product, and audit
0.5 Formal conventions, cryptographic notation, and reading criteria

1. byLAEV Foundations: Professional Philosophy and Methodology Applied to DLBW

1.1 Principle of publicly verifiable integrity: complete documentation, reproducibility, and auditability
1.2 Principle of sufficient minimal traceability: technical evidence without disclosure of sensitive material
1.3 Principle of technical non-simulacrum: exclusion of non-enforceable or non-demonstrable claims
1.4 Principle of structural responsibility: strict separation between design, operation, and independent verification
1.5 Principle of methodological presence: continuous recording of decisions, changes, and versions (byLAEV methodology)
1.6 Principle of systemic–industrial design: coherence between user experience and real cryptographic constraints
1.7 Criterion of operational truth: formal distinction between usage rules, policies, and technical enforcement

2. Formal Definitions and Technical Glossary

2.1 DLBW (Deterministic License-Based Wallet): normative definition
2.2 License: cryptographic identity, operational quota, policy, and validity regime
2.3 Device: verifiable cryptographic identity (DeviceID) and optional hardware evidence (attestation)
2.4 License registry: event-sourcing-based ledger and deterministic verification
2.5 Event typology: GENESIS, ACTIVATE, DEACTIVATE, ROTATE, ALERT
2.6 Bitcoin anchoring: cryptographic commitments, Merkle root, and inclusion proofs
2.7 Alert system: metrics, accumulated severity, and reason codes
2.8 Governance: keys, quorum, revocation, and re-issuance processes
2.9 Enforceability: minimum technical conditions to guarantee “N devices”

3. Formal Problem Statement

3.1 Structural limitation: inherent copyability of seeds and private keys
3.2 Functional objective: controlled correspondence between a license and a finite set of authorized devices
3.3 Operational objective: detection, recording, and traceability of out-of-policy attempts
3.4 Economic and product objective: issuance, delivery, and lifecycle management of usage licenses
3.5 Audit objective: generation of publicly verifiable evidence without custody of secrets

4. Threat Model

4.1 Primary threats: seed cloning, installation duplication, replay attacks, impersonation
4.2 Secondary threats: DeviceID exfiltration, event manipulation, malicious indexers
4.3 Systemic threats: user coercion, device loss, actor collusion
4.4 Explicit security assumptions
4.5 Mitigation strategies classified by severity and impact

5. System Requirements Specification (SRS)

5.1 Functional requirements (FR): activation, quota control, licensed operation
5.2 Non-functional requirements (NFR): availability, latency, cost, scalability, resilience
5.3 Security requirements: authenticity, integrity, non-repudiation, auditability
5.4 Privacy requirements: data minimization, pseudonymization, explicit consent
5.5 Interoperability requirements: HD wallet compatibility and existing standards

6. Reference Architecture of the DLBW System

6.1 Functional layers: wallet client, event registry, distributed indexing, Bitcoin anchoring
6.2 Core identities: LicenseID and DeviceID
6.3 Operational flows: installation, activation, operation, revocation, replacement
6.4 Formal license states: active, suspended, revoked, quota exhausted
6.5 Operational decentralization: registry consensus mechanisms

7. License Identity (LicenseID) and GENESIS Event

7.1 Cryptographic construction of LicenseID: hashing, versioning, metadata
7.2 GENESIS event: initial quota, policy, governance keys, and parameters
7.3 License representation for issuance and delivery
7.4 Critical conceptual separation: control credential vs. registered state
7.5 Validity regimes: perpetual and temporal licenses, expiration mechanisms

8. Device Identity (DeviceID)

8.1 Local generation of key pairs and recommended non-exportability
8.2 Deterministic construction of DeviceID
8.3 Optional attestation: classification of trust levels by platform

8.4 Fingerprinting risks and mitigation strategies
8.5 Uniqueness guarantees and collision analysis

9. Decentralized License Registry (Event-Sourcing Ledger)

9.1 Formal model: signed events and deterministic state derivation
9.2 Event validation and acceptance rules
9.3 Conflict resolution, ordering, and consistency
9.4 Multiple indexers and independent verification
9.5 Registry persistence, replication, and availability

10. Device Activation and Quota Enforcement

10.1 ACTIVATE event: controlled device onboarding under a license
10.2 Quota policies: maximum limits, reservations, and contingencies
10.3 Enforceability conditions: effective denial of out-of-policy operations
10.4 DEACTIVATE event: voluntary and security-driven deactivation
10.5 Device replacement (swap): formal procedure
10.6 Recovery mechanisms without degrading quota enforcement

11. Wallet Operation Under License Regime

11.1 Definition of critical operations and preconditions
11.2 Authorization proofs: verification of active DeviceID
11.3 Session policies, periodic revalidation, and rate control
11.4 HD compatibility: key derivation without license model violation
11.5 Local secret management, backups, and rotation

12. Alert System and Risk Scoring

12.1 ALERT event: formal definition, formats, and severity
12.2 Scoring models: weighting functions, time windows, and thresholds
12.3 Policy-driven automated responses: suspension and escalation
12.4 Technical evidence: traceability of unauthorized attempts
12.5 Alert evaluation: false-positive and false-negative analysis

13. Cryptographic Anchoring on the Bitcoin Network

13.1 Periodic commitments: event Merkle roots and optimal anchoring frequency
13.2 Inclusion proofs and independent external verification
13.3 Cost analysis and batching strategies
13.4 Immutability and timestamp guarantees: scope and limitations
13.5 Documentary evidence associated exclusively with the license wallet

14. Governance and License Lifecycle Administration

14.1 Governance key structure: multisig, quorum, and roles
14.2 ROTATE event: policy and key updates
14.3 REVOCATION event: definitive revocation and objective criteria
14.4 Controlled re-issuance and migration
14.5 Auditor independence and external verification processes

15. Privacy, Security, and Compliance

15.1 Data minimization principle: strict limits on recorded information
15.2 Systematic pseudonymization of LicenseID and DeviceID
15.3 Metadata protection: risks and countermeasures
15.4 Technical controls: anti-replay, anti-forgery, anti-tamper
15.5 Audit readiness without custody of sensitive information

16. Reference Implementation

16.1 Message formats (JSON/CBOR), versioning, and compatibility
16.2 Cryptographic library selection and security considerations
16.3 Client requirements: mobile, desktop, and specialized hardware
16.4 Indexer requirements: availability, verification, and caching
16.5 Testing strategies: unit, integration, and adversarial testing

17. Metrics and Evaluation Criteria

17.1 Licensing KPIs: activations, revocations, replacements
17.2 Security KPIs: rejected attempts, accumulated severity, response times
17.3 Audit KPIs: independent verifications and anchoring latency
17.4 Experience KPIs: operational friction, recovery, and support
17.5 Standard reporting template for stakeholders

18. Formal Conclusions

18.1 Technically and empirically enforceable assertions
18.2 Assertions explicitly excluded for lack of enforceability
18.3 Final definition of DLBW as a formal wallet class

Annexes

A. Reason-code catalog for ALERT events
B. Formal LicenseID state diagram
C. Technical evidence and audit templates
D. Attack vectors and mitigation matrices
E. Interoperability notes with HD standards