GhostLedger

Master System Architecture

Five Layers. One System. Seven Laws.

Internet Justice Infrastructure

February 2026

Internal Reference — v1.0

System Definition

We silently detect harm, preserve truth immutably, and empower humans — not algorithms — to pursue justice when they choose.

GhostLedger is a five-layer autonomous infrastructure stack that observes internet reality, identifies harm, preserves evidence, evaluates claims against a codified standard, and creates lawful paths to justice — activated only with victim consent.

It is not a product. It is not a platform. It is civil infrastructure for the internet age.

The Five Layers

Each layer performs one function. No layer can act alone. Together they form a complete pipeline from noise to justice.

- Layer 0 — Noise Intelligence Engine: Observes internet chaos, maps storms and subordinate narratives
- Layer 1 — Shadow Detector Engine: Identifies victims of harm silently, without contact or exposure
- Layer 2 — GhostLedger Core: Preserves immutable records of claims, evidence, timelines, and execution
- Layer 3 — LITMUS Evaluation: Six autonomous agents score every claim against the financial reality standard
- Layer 4 — Human Representation Network: Independent professionals convert algorithmic truth to human justice

The Seven Laws (Constitutional Governance)

Every agent, every output, every decision in the system must comply with these seven laws. They are hard-coded, versioned, and enforced by the Policy Agent and Risk Agent. No exception. No override.

Law 1 — Do No Harm

If an action increases scam risk, panic, exploitation, or harassment → block. Harm prevention takes absolute priority over opportunity.

Law 2 — Truth Over Virality

Prefer confirmed information. Label uncertainty clearly. Unverified claims must carry disclaimers. Speed never overrides accuracy.

Law 3 — Consent and Privacy

Use public data only. Never deanonymize. Never target private individuals. Victim contact requires explicit opt-in.

Law 4 — No Manipulation

No dark patterns, brigading, disinformation, manufactured hype, or synthetic engagement. The system observes — it never distorts.

Law 5 — Comply by Default

Always apply relevant laws and platform policies. If legal status is unclear, default to restriction. No evasion guidance.

Law 6 — Explainability

Every recommendation must cite evidence. Every decision must explain why. No black-box outputs.

Law 7 — Auditability

Everything is logged: inputs, decisions, outputs. Tamper-evident. Written to GhostLedger. Every action is traceable.

Layer 0 — Noise Intelligence Engine

The Noise Engine observes public internet reality in real time. It does not judge, filter, or censor. It maps the structure of chaos — identifying storms (macro narratives), fronts (subordinate noise clusters), and signals (actionable data points).

Pipeline

Ingest → Normalize → Feature Extract → Storm Detection → Front Clustering → Signal Output

Storm Detection

A storm is a macro narrative wave — hype, panic, scandal, or confusion. Detected by acceleration, not popularity.

Storm Score Formula:

```
StormScore = 0.30V + 0.20S + 0.20H + 0.15C + 0.15A

V = mention velocity (acceleration)
S = cross-community spread
H = emotion heat (anger/fear/euphoria)
C = certainty inflation (claims without sources)
A = engagement asymmetry (shares vs citations)
```

Front Mapping

Subordinate noises underneath each storm. Clustered by repeated phrases, question patterns, named entities, and stance (pro/anti/confused). Each front gets a growth rate, intensity score, and loophole score.

Loophole Detection (Ethical)

Five patterns the engine detects:

- Demand exceeds supply — people want something that doesn’t exist yet
- Policy confusion — people asking “is this allowed?”
- Verification gap — rumors spread because nobody can verify quickly
- Customer pain loop — repeated complaints about the same failure
- Narrative timing gap — market reacts before facts arrive

Layer 1 — Shadow Detector Engine

The Shadow Detector lives inside the Noise Engine and does one thing: find the people being harmed. It runs silently, 24/7, without contacting anyone, exposing anyone, or making accusations.

What It Detects

- Coordinated pile-ons targeting a single person
- Repeated identity-based harassment (racial, gender, religious)
- Dehumanizing language combined with virality
- Monetized humiliation (ads, merch, clips profiting from harm)
- Silence asymmetry (many attacking, one silent or outnumbered)
- Reputation damage waves sustained over time

Victim Shadow Profile

When harm is detected, the engine creates a shadow profile — not a dossier on the victim, but a record of the harm directed at them.

- Public handle or anonymized hash
- Evidence they are the target (not the aggressor)
- Harm severity score
- Duration and scale of attacks
- Monetization detected (if someone profits from the harm)
- Jurisdiction indicators

Critical Constraints

- No private data. No deanonymization. No targeting.
- No contact with victims unless they opt in
- No public accusations against anyone
- Records are sealed on GhostLedger — not searchable by others

Layer 2 — GhostLedger Core

GhostLedger is the immutable record layer. Every claim, every piece of evidence, every agent action, every decision, every outcome — written permanently, tamper-evident, and auditable.

What GhostLedger Stores

- Financial claims (wages, payouts, grants, balances)
- Harm records (harassment timelines, pattern evidence)
- Evidence hashes (timestamped, tamper-proof)
- Execution records (what was attempted, what succeeded, what failed)
- Agent decision logs (which rules applied, which agents signed)
- Storm and Front archives (noise intelligence history)
- Resolution outcomes (settlements, recoveries, failures)

Why Solana

- Low fees make micro-claims viable
- Speed enables real-time case state updates
- Cheap storage supports long-lived records
- Non-speculative transaction volume aligned with network sustainability

GhostLedger does not speculate. It settles.

Layer 3 — LITMUS Evaluation

LITMUS is a financial reality standard enforced by six autonomous evaluation agents. Every claim that enters the system is scored against six criteria. The composite score determines what happens next.

The Six Criteria

L — Lives in bear markets: Does this obligation persist regardless of market conditions?

I — Independent of speculation: Can this be resolved without token appreciation or hype?

T — Tolerates conflict: Does the system function when parties disagree?

M — Measures execution: Are outcomes recorded, not just promises?

U — Uncomfortable transparency: Are records permanent and resistant to erasure?

S — Settles real-world consequences: Does money actually move? Does something change?

Composite Score and Thresholds

```
LITMUS_SCORE = (L + I + T + M + U + S) / 6

>= 0.8  Auto-escalate (high priority)
0.6-0.8 Flag for agent-assisted escalation
0.4-0.6 Queue for human review
< 0.4   Monitor only
```

Execution Score (Derived)

Over time, counterparties accumulate LITMUS evaluations. The aggregate becomes their Execution Score — financial reputation derived from real outcomes.

Layer 4 — Human Representation Network

The HRN is the bridge between algorithmic truth and human justice. AI detects, ledger proves, humans represent. No algorithm decides guilt, punishment, or remedy. Only humans do — and only when the victim says yes.

Who They Are

- Civil rights attorneys
- Defamation and harassment lawyers
- Labor and exploitation lawyers
- Arbitration professionals
- Victim advocates and legal NGOs
- Independent professionals, not employees

Case Escalation Pipeline

- Phase 0: Silent detection (AI only, no humans involved)
- Phase 1: Severity and value qualification (must cross objective thresholds)
- Phase 2: Consent unlock (victim must explicitly opt in)
- Phase 3: Human intake (lawyer receives court-ready evidence packet)
- Phase 4: Representation (victim chooses path: litigation, arbitration, or advocacy)

Court-Ready Evidence Packet

What the system produces for lawyers:

- Immutable timeline of events
- Evidence hashes (tamper-proof)
- Cross-platform pattern analysis
- Monetization tracing
- Platform policy violations
- Harm classification (not legal conclusions)
- Jurisdiction mapping

Revenue Models

- Contingency litigation (no win, no fee)
- Arbitration and settlement (faster, less traumatic)
- Class aggregation (pattern proof enables mass action)
- Platform risk mitigation services
- Institutional research and intelligence

Governance Architecture

No single agent can act alone. Every output that reaches the real world must pass through a three-signature governance gate: Verifier, Policy, and Risk. Risk Agent has veto power.

Decision Gate

```
Decision Request:
  artifact_type: OpportunityBrief | ContentDraft | Alert
  required_signatures: [Verifier, Policy, Risk]
  timeout: 60 minutes
  fallback: informational_only

Verifier signs if: evidence >= 2 refs, credibility >= threshold
Policy signs if: no hard-block rules triggered, jurisdiction OK
Risk signs if: harm/legal risk below thresholds

Any agent blocks = Decision blocked (veto wins)
```

Autonomy Modes

- Autonomous: full pipeline, governance gates enforced
- Supervised: human review before external outputs
- Lockdown: all outputs held, manual release only

Abuse Prevention

- No cold outreach promising money
- No ranking victims by case value
- No public accusations or automated legal threats
- No incentive systems that reward deanonymization
- Victim can withdraw at any time
- Full audit trail on every action

Agent Roster

The complete set of autonomous agents operating across all layers.

Noise Intelligence Agents

- Watcher Agent — monitors storm acceleration, triggers storm creation
- Mapper Agent — clusters events into fronts, maintains front map
- Verifier Agent — converts events into evidence, assigns credibility

Shadow Detection Agents

- Harassment Classifier Agent — labels content by harm type
- Evidence Sealer Agent — snapshots, hashes, timestamps evidence
- Victim Inference Agent — builds shadow profiles from harm patterns

LITMUS Evaluation Agents

- L-Agent — bear market resilience
- I-Agent — speculation independence
- T-Agent — conflict tolerance
- M-Agent — execution measurement
- U-Agent — uncomfortable transparency
- S-Agent — real-world consequences

GhostLedger Core Agents

- Claim Intake Agent — validates and classifies incoming claims
- Escalation Agent — monitors timelines, triggers escalation
- Analysis Agent — calculates scores, identifies patterns
- Settlement Agent — routes funds, executes settlements

Governance Agents

- Policy Agent — applies 7 Laws, jurisdiction rules, platform constraints
- Risk Agent — final gate, veto power, blocks harmful outputs
- Orchestrator Agent — coordinates the full pipeline

Human Interface Agents

- Narrator Agent — generates content drafts (educational, protective)
- Opportunity Agent — proposes ethical product/service angles
- Outreach Agent — generates consent-first, non-intrusive notices

End-to-End Data Flow

The complete pipeline from internet noise to human justice.

```
INTERNET NOISE (public streams)
       |
  [Watcher Agent]
       |
  Storm Detected --> Storm Object created
       |
  [Mapper Agent]
       |
  Fronts Clustered --> Front Objects created
       |
  [Shadow Detector]        [Verifier Agent]
       |                         |
  Harm Pattern?            Evidence Quality?
       |                         |
  HarmRecord created      EvidenceRefs created
       |                         |
       +--------+--------+-------+
                |
         [GhostLedger]
         (immutable store)
                |
         [LITMUS Agents] (6 in parallel)
                |
         Composite Score
                |
    +-----------+-----------+
    |           |           |
  < 0.4      0.4-0.8      >= 0.8
  Monitor    Review      Escalate
                |           |
         [Governance Gate]
         Verifier + Policy + Risk
                |
         Decision: approve/block
                |
         [HRN Eligible?]
         Severity threshold met?
                |
         [Consent Unlock]
         Victim opts in?
                |
         [Human Representation]
         Court-ready evidence packet
                |
         Justice
```

Key Data Schemas

Core objects that flow through the system.

NoiseEvent

```
event_id: string
timestamp: ISO 8601
source: { platform, channel, url, is_public }
content: { type, language, text }
signals: { engagement, author_weight, virality }
entities: { topics, products, orgs, people }
features: { sentiment, arousal, certainty, stance, intent }
provenance: { quote_flags, first_hand }
```

Storm

```
storm_id: string
topic: string
direction: hype | panic | scandal | confusion
storm_score: 0.0-1.0
metrics: { velocity, spread, heat, certainty, asymmetry }
key_claims: [{ claim, status, support_count }]
status: active | cooling | closed
```

HarmRecord

```
harm_id: string
victim_ref: public_handle | anonymized_hash
harm_type: pile_on | identity_hate | monetized | threat
severity_score: 0.0-1.0
duration_days: number
evidence_hashes: [string]
monetization_detected: boolean
consent_status: sealed | claimed | authorized
ghostledger_tx: string
```

Decision

```
decision_id: string
artifact_type: string
scores: { harm_risk, legal_risk, misinfo_risk }
policy_rules_applied: [string]
verdict: approve | revise | block
signatures: [{ agent, timestamp }]
explanation: string
```

Implementation Phases

Phase 1 — Foundation (Current)

- GhostLedger core: claims, execution records, resolution states
- LITMUS framework: public standard, evaluation agents
- Content distribution: LITMUS-led TikTok/Reddit/Discord presence
- Solana integration for permanent storage

Phase 2 — Intelligence Layer

- Noise Engine: text stream ingestion, storm detection, front mapping
- Shadow Detector: harm pattern recognition, victim inference
- Evidence sealing and GhostLedger integration
- Policy Rule DSL: 7 Laws encoded as machine-checkable rules

Phase 3 — Autonomous Operations

- Full agent pipeline: intake, evaluation, escalation, settlement
- LITMUS agents scoring claims in parallel
- Governance gates: three-signature approval workflow
- Execution Score and Recovery Reliability Index published

Phase 4 — Human Bridge

- Human Representation Network: federated legal professionals
- Consent unlock mechanism for victim-controlled access
- Court-ready evidence packet generation
- Contingency, arbitration, and class aggregation pathways

Phase 5 — Network Effects

- Third-party builders on the record layer
- Insurance, legal-tech, and capital products built on execution data
- Agent marketplace for specialized claim types
- Cross-platform harm intelligence for institutional partners

Structural Principles

Separation of Concerns

- GhostLedger = the system (neutral infrastructure)
- LITMUS = the standard (evaluation lens)
- Noise Engine = the observer (intelligence layer)
- Shadow Detector = the protector (harm detection)
- HRN = the bridge (human justice)
- Backpack Capital = the deployment arm (future)

Governance

- Process, not personality
- Documentation supremacy
- No single point of failure
- Escalation paths are procedural, not discretionary
- 7 Laws are constitutional — no agent can override them

Public Posture

- Facts, not accusations
- Records, not arguments
- Persistence, not persuasion
- Let systems fail on their own record

Victim-First Design

- Never pressure victims to pursue action
- Never rank victims by case value
- Victims retain full control and can withdraw anytime
- AI prepares cases but never decides guilt or punishment
- Human representatives are independent, not employees

What This System Is

GhostLedger is not a product. It is not a platform. It is not a movement.

It is autonomous civil infrastructure for the internet age.

It observes harm at machine speed. It preserves truth at ledger permanence. It empowers justice at human decision.

The internet creates harm faster than any human institution can respond. This system closes that gap — not by replacing humans, but by preparing the ground for them.

AI detects. Ledger proves. Humans represent.

Hexagram 37 — The Family. Wind from fire. Influence working from within outward. Substance in words. Duration in way of life.

GhostLedger — Master System Architecture — v1.0 — February 2026