# **CLAW Protocol — Whitepaper v1.0**

### **Civitas Law for a Programmable World**

## **0 Executive Summary**

CLAW (Civitas Law) is a decentralized, privacy-preserving legal-automation protocol.

It replaces administrative trust with verifiable, cryptographic proof by combining:

* Aztec Network – private clause execution using zero-knowledge proofs.
* LitVM – encryption and conditional key release for evidence and documents.
* Base / Polygon / Ethereum – public settlement, registry, and payment rails.
* Bitcoin Daily Save – immutable anchoring of all registry roots.
* Coinbase Pay / Commerce – fiat ↔ USDC on/off-ramp.
* THORChain – native BTC/ETH/ATOM cross-chain liquidity.

Layered on top are two DAOs and a treasury token (PCred) that align lawyers, nodes, affiliates, and users into one verifiable ecosystem.

## **1 Motivation & Principles**

Administrative law depends on opaque intermediaries. CLAW re-implements legal process as transparent state machines that anyone can audit.

Guiding Principles

* Privacy by default; proofs public, payloads private.
* Voluntary participation; credentialed governance.
* One-way integrity: nothing can be deleted or retroactively changed once anchored to Bitcoin.
* Jurisdictional compliance via bar-verified authorship and zk-KYC.

## **2 System Overview**

Three core layers govern all activity:

1. Clause Layer – bar-verified clauses published as NFT-style artifacts with jurisdictional metadata.
2. Proof Layer – attested executions, timestamps, and ZK proofs of performance or breach.
3. Governance Layer – lawyer + node DAOs that confirm integrity, manage upgrades, and arbitrate disputes.

Daily Merkle roots of all proofs are anchored to Bitcoin.

## **3 Architecture**

### **3.1 Anchors & Public Record**

* Bitcoin Daily Save – one TX per day; cost ≈ 20 000 sats.
* Dash ChainLocks / Arweave Mirror – optional fast-finality and archival redundancy.

### **3.2 Settlement Chains**

* Base (primary) + Polygon (low fee) + Ethereum (fallback).
* Assets: USDC and PCred.
* NFT (ERC-721) for clauses; ERC-1155 for proof receipts; ERC-20 for PCred.

### **3.3 Privacy & Encryption**

* Aztec executes clauses privately and proves compliance without revealing data.
* LitVM stores encrypted keys and releases them only when contract conditions are satisfied.

### **3.4 Payments & Liquidity**

* Coinbase Pay/Commerce – fiat ↔ USDC; chargeback mitigation via LitVM time-locks.
* THORChain – streaming swaps for BTC ⇄ USDC ⇄ other assets; fallback to DEXes on Base/Polygon.
* Routing Controller – selects optimal path (asset, size, geography, compliance) and records signed route receipt.

### **3.5 Data & Storage**

* Encrypted docs on IPFS/Filecoin; LitVM controls keys.
* Public chain stores hashes only; optional Arweave mirror for redacted cases.

### **3.6 Identity & Credentials**

* Wallet-first DID/VC.
* zk-KYC for lawyers & users.
* Attestor nodes sign AI cross-checks (GPT / Claude / Gemini parity).

## **4 Core Modules**

### **4.1 Clause Registry**

Lawyers publish reusable, jurisdiction-aware clauses; metadata includes bar ID, disclaimer, hash lineage.

Marketplace ranks by adoption & validator feedback.

### **4.2 Proof Engine**

Generates attestations for service, performance, oracle events, and disputes.

All proofs hashed to Base → Bitcoin Daily Save.

### **4.3 Dispute Resolver**

Supports single validator → panel → appeal tiers.

Evidence encrypted; decisions public as hash + outcome code.

### **4.4 Treasury & PCred**

* PCred = accounting token (ERC-20) for protocol fees + rewards.
* Fully reserved (USDC/BTC); mint/burn on lifecycle events.
* Reserve attestations → Bahrain CBB alignment.

## **5 Legal & Jurisdictional Design**

### **5.1 Bar Verification**

Each lawyer holds zk-verifiable credential tied to jurisdiction.

### **5.2 Disclaimers & UPL Protection**

Clauses carry metadata: “not personal legal advice; verify jurisdictional fit.”

### **5.3 Clause Schema Governance**

Changes require Lawyer DAO super-majority vote.

### **5.4 Lawyer DAO**

* Membership – bar-verified + 1 000 PCred-L stake.
* Rewards – share of registration and execution fees (20 % average).
* Voting – credential weight + reputation score; hard cap per member.
* Slashing – fraud, UPL risk, defective clauses; appeal to mixed panel.

## **6 Privacy & Encryption Framework**

Aztec handles private clause state; LitVM enforces access conditions.

Selective disclosure = “prove you complied” without revealing content.

All evidence keys, payments, and decisions log encrypted proofs → public hash.

## **7 Economic Model**

### **7.1 Fee Buckets (per event)**

| **Allocation** | **% of Protocol Fee** |
| --- | --- |
| Validator pool | 40 % |
| Lawyer DAO | 20 % |
| Treasury reserve | 20 % |
| Attestors | 10 % |
| Affiliates | 10 % |

### **7.2 Example**

User funds $10 000 escrow → 1 % fee = $100.

Distribution = $40 V + $20 L + $20 T + $10 A + $10 Aff.

Escrow release = $9 900.

### **7.3 Bitcoin Daily Save Cost**

≈ $5 000 / yr (0.073 BTC) covered by 0.05 % anchor surcharge.

### **7.4 Routing Math**

Route Cost = Amount × (slippage + network fee) ≤ 0.7 %.

Router earns 0.1 % bps → Node DAO + Treasury.

## **8 Security & Verification**

* Privacy: Aztec + LitVM = confidential payloads.
* Integrity: multi-model attestors; Merkle root anchoring.
* Liquidity risk: THORChain streaming swaps + caps.
* On-ramp risk: LitVM time-locks for card/ACH funds.
* Compliance: OFAC/AML at on-ramp + zk-KYC inside.
* Slashing & Bonds:  
    
    Lawyer DAO stake → PCred-L slash on fraud.  
    
    Node DAO stake → PCred-N slash on downtime or conflict.  
    
    User micro-bond → spam deterrent.  
    
    Insurance fund → covers rare reversals.

## **9 Governance & Participation**

### **9.1 Founding Clause Authors**

Seed the registry and set standards.

### **9.2 Validators (Node DAO Tier A–C)**

Stake PCred-N; earn event fees + routing bps; subject to SLA metrics.

### **9.3 Attestors**

AI model cross-checks; signed proofs; 10 % fee share.

### **9.4 Appeals**

Multi-jurisdictional panel → final decision hash → Bitcoin anchor.

### **9.5 Node DAO**

Governance for validators/executors/attestors.

Votes on routing policies, gas budgets, model lists.

## **10 Go-to-Market Strategy**

### **10.1 Phase 1 – Seed (0–3 mo)**

* Recruit 20–50 Lawyer DAO members.
* Pilot NDA & HR clauses.
* Launch Coinbase on-ramp + Daily Save MVP.

### **10.2 Phase 2 – Private Disputes (3–6 mo)**

* Arbitration templates; Node DAO live; THORChain routing.

### **10.3 Phase 3 – Institutional (6–12 mo)**

* Law-firm integrations; Litigation-finance tranches; Dashboard Explorer.

### **10.4 Phase 4 – Public Scale (12 mo +)**

* Multi-jurisdiction; insurance + parametric use cases.

### **10.5 Metrics**

Case volume, avg decision time, slashing rate, Daily Save continuity, affiliate ROI.

### **10.6 Affiliate Programs**

* Lawyer Affiliate: recruit bar-verified authors; 10 % trailing share 12 mo.
* Case Affiliate: bring cases; 10 % fee + 2 bps escrow (90 days).
* Node Affiliate: recruit validators; 8 % reward share 6 mo.
* Integrator Affiliate: SDK partners; 15–25 % rev share.  
    
   All IDs recorded in proof receipts; payouts in USDC or PCred.

## **11 Use Cases (Condensed Catalog)**

A Legal Automation: Employment / NDAs / IP Licensing / Procurement.

B Disputes: Arbitration / Small Claims / Defamation Finance.

C Governance: DAO Policies / Board Resolutions.

D Accountability: Whistleblower / Public Timeline Anchors.

E Commerce & Assets: Escrow / Cross-Chain Payout / Insurance.

F Compliance: Lawyer Gating / zk-Accreditation.

G Developer: ClauseBuddy AI + APIs for HR and Legal ops.

## **12 Mathematical Reconciliation (Plain English)**

| **Symbol** | **Meaning** |
| --- | --- |
| P | total escrow value |
| f\_c | protocol fee (≈ 1 %) |
| f\_a | affiliate fee |
| f\_r | routing cost |
| f\_b | Bitcoin anchor cost |

Total deduction = P × (f\_c + f\_a + f\_r + f\_b)

Net to parties = P − deduction.

All sub-shares sum to 100 %.

Treasury net = Σ (inflows − rewards − anchors − ops).

One Merkle root/day → Bitcoin; proof integrity = 100 %.

## **13 Compliance & Risk**

* Stable-unit: CBB reserve policy, redemption terms, audit cadence.
* KYC/AML: Coinbase on-ramp; zk-KYC internally.
* UPL: lawyer-only registration; disclaimers.
* Data: encrypted storage; lawful access logs.

## **14 Roadmap (Technical)**

1. Registry + Coinbase integration MVP.
2. Aztec private execution + LitVM key logic.
3. THORChain router + streaming swap planner.
4. Escrow v1 + appeal module.
5. Public Explorer + Bitcoin hash index.
6. ClauseBuddy AI tooling.
7. Audits & reserve attestations.

## **15 Conclusion**

CLAW turns law into code without losing ethics or privacy.

It links jurisdictional expertise (Lawyer DAO) with verifiable execution (Node DAO), public transparency (Base + Bitcoin), and private fairness (Aztec + LitVM).

Through clear math and immutable anchoring, every legal interaction becomes provably honest, compliant, and efficient.

## **Appendix A Glossary**

PCred – Proof Credit token for fees and rewards.

Daily Save – 24 h Merkle root anchoring to Bitcoin.

Route Receipt – signed record of payment path.

ClauseBuddy – AI assistant for drafting and metadata.

## **Appendix B Example Flow (NDA Case)**

1 Lawyer registers clause ($100 fee → 50/30/10/10).

2 User funds $10 000 escrow (via Coinbase).

3 Aztec executes privately; LitVM holds keys.

4 Validator decides; funds released; hash → Base → Bitcoin.

5 Affiliate earns $10; all balances sum exactly.

## **Appendix C Version History**

* v1.0 (2025-10-18) – Full integration of Lawyer DAO, Node DAO, Affiliate Programs, routing math, and proof flows.
* v0.12 – DAO modules added.
* v0.11 – THORChain / Coinbase integration, expanded use cases.
* v0.10 – Aztec / LitVM privacy stack + Daily Save anchoring.

Prepared by Anthem Hayek Blanchard — Founder, CLAW Protocol

Contact: [anthemhayek@me.com](mailto:anthemhayek@me.com) ; X.com: @anthemhayek