

ClawdSure: Telematics-Based Insurance for AI Agents

Concept Note & Proof of Attestation Chain

Prepared for: Greenlight Re

Prepared by: Mark Musson, Founder, Kryptoplus Labs (krypto.plus)

Date: February 2026

Version: 2.0

Executive Summary

AI agents are deploying at scale. They manage infrastructure, hold credentials, execute code, access APIs, and interact with financial systems — autonomously, 24/7. There is no insurance product for when they get compromised.

ClawdSure is a continuous security attestation system — a **telematics box for AI agents** — that produces the verifiable behavioural monitoring required to underwrite agent breach insurance for autonomous AI deployments.

The Wedge: We start with OpenClaw — the first viral personal AI agent framework, and also the most unsecured. Our hypothesis is that we can solve for making OpenClaw instances insurable and prove this with our first product. The TAM is the millions of OpenClaw instances that will explode in the coming months. Once validated, we expand to Langchain, Vercel AI SDK, and other agent frameworks.

The Edge — Yield on Float: Premiums collected in USDT are routed to Morpho vaults via HyperSend (Kryptoplus infrastructure), earning 6-12% APY. This transforms marginal underwriting into a profitable float business.

The Ask: Quota share reinsurance partnership with Greenlight Re.

Why Now

The Supply Chain Attack That Proves the Need

In February 2026, the most downloaded skill on ClawHub (the package manager for AI agent plugins) was found to be a malware delivery vehicle. The attack:

- Used a fake dependency to deliver an obfuscated payload
- Stripped macOS quarantine flags to bypass Gatekeeper
- Was viewed 10.7 million times before discovery
- Affected an unknown number of OpenClaw instances

There was no insurance. No attestation. No way for operators to prove they weren't compromised.

The OpenClaw Opportunity

OpenClaw is the fastest-growing personal AI agent framework:

- Open source, viral adoption
- Agents with tool access, API credentials, execution capabilities
- Gateway-connected, channel-enabled (Telegram, Discord, WhatsApp, Slack)
- Running on user hardware and cloud VPS
- Holding credentials worth protecting
- **No built-in security attestation or insurance**

Year	Estimated Autonomous Agents	Growth
2024	100K	—
2025	500K	400%
2026	2M	300%
2027	5M+	150%
2028	10M+	100%

How ClawdSure Works

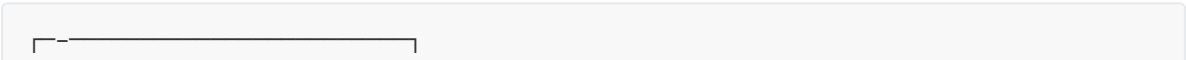
The Telematics Analogy

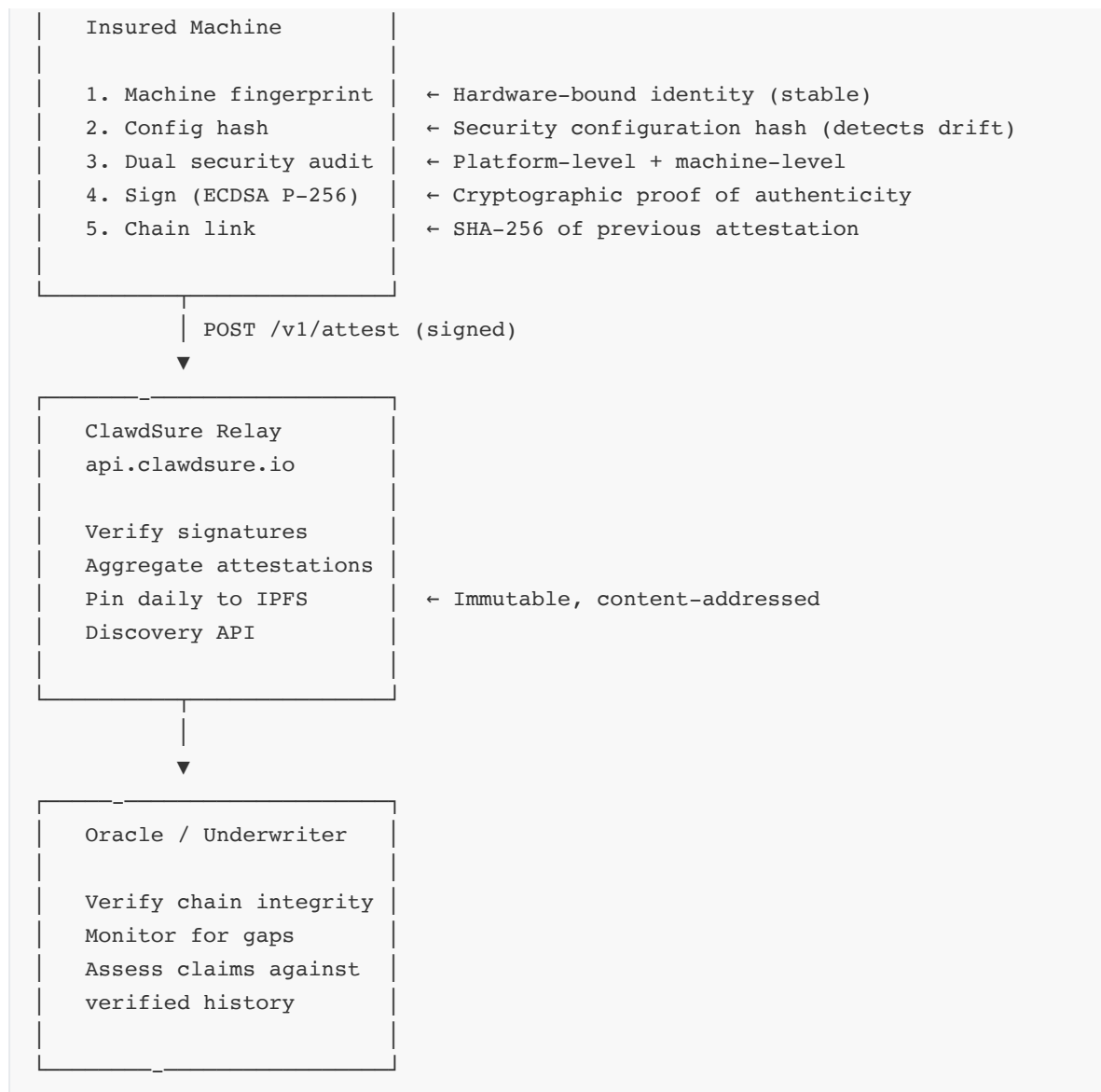
Mark Musson previously built and sold a dynamic by-the-second motor pricing MGA to AON, reaching £40m GWP. The core insight is identical:

Motor Insurance	AI Agent Insurance
Telematics box in the car	ClawdSure on the machine
Driving data (speed, braking, location)	Attestation data (fingerprint, config, audit)
Continuous telemetry → risk scoring	Continuous attestation → chain integrity
Good driving = lower premium	Unbroken chain = valid coverage
Crash event assessed against driving data	Security incident assessed against attestation chain
Data stored with insurer	Data pinned to IPFS (public, verifiable)

The key insight: Like motor telematics, the attestation chain determines **eligibility** for claims. When an incident occurs, was the chain valid at the time? Then the claim can be assessed. If the chain was broken, coverage was void. The difference: IPFS gives us a **public, immutable, content-addressed** record. No dispute about what was attested and when.

Architecture





No IPFS accounts needed on the insured machine. The relay handles all pinning.

No human intervention. Attestation runs daily via automated scheduler.

Portable. Works on macOS, Linux, WSL. Dependencies: `openssl`, `jq`, `curl`.

What Gets Attested (Dual Audit)

Layer 1: Platform Security Audit (`audit_native` hash)

- Gateway exposure and authentication mode
- Channel policies (DM, group access controls)
- Browser and elevated execution settings
- Attack surface summary

Layer 2: Machine Security Audit (`audit_machine` hash)

- Filesystem permissions on state, config, and credentials directories
- Synced folder detection (Dropbox/iCloud/OneDrive/Google Drive exposure)
- SUID/SGID and world-writable file scanning
- Firewall status (macOS/ufw/iptables/nftables)

- Listening port inventory
- Installed skills inventory and pattern scanning for malicious payloads
- Operational coherence (model configuration consistency)

Both layers are hashed independently and included in every attestation. A change in either hash between attestations signals drift.

Proof of Concept: Live Attestation Chain

The following chain was generated from a live OpenClaw deployment on 8 February 2026.

Agent Identity

- **Agent ID:** CLWD-3F8B0233
- **Machine:** Darwin arm64, OpenClaw 2026.2.6-3
- **Machine Fingerprint:** 14d547ddde1cd179... (SHA-256 of hardware UUID)
- **Config Hash:** c05ff9b7ee6b5801... (SHA-256 of security-relevant configuration)

Genesis Attestation (#1 — Enrollment)

```
{
  "v": 1,
  "seq": 1,
  "prev": "genesis",
  "ts": "2026-02-08T07:01:29Z",
  "agent": "CLWD-3F8B0233",
  "fingerprint": {
    "machine":
"14d547ddde1cd179aacdf3afc702517c44b637973156c84aa885ef041eea43eb",
    "config": "c05ff9b7ee6b5801f502c07468ad9745aa1086d97eea9a051d5e250d534f47e0",
    "openclaw": "2026.2.6-3",
    "os": "Darwin",
    "arch": "arm64"
  },
  "result": "PASS",
  "sig": "MEUCIQCoFMxAaWkILYg41wQhXyoljc+kDIbbS8x6zRA1BUGAHwIg..."
}
```

Attestation #6 (Latest — With Dual Audit)

```
{
  "v": 1,
  "seq": 6,
  "prev": "c6107377d55f9ca5aa08093bb989069b9bdf7a02ff79c0eca2fc8cef23224f8b",
  "ts": "2026-02-09T09:30:09Z",
  "agent": "CLWD-3F8B0233",
  "fingerprint": {
    "machine":
"14d547ddde1cd179aacdf3afc702517c44b637973156c84aa885ef041eea43eb",
    "config": "c05ff9b7ee6b5801f502c07468ad9745aa1086d97eea9a051d5e250d534f47e0",

```

```

    "openclaw": "2026.2.6-3",
    "os": "Darwin",
    "arch": "arm64"
  },
  "audit_native":
"ffb61a696bd26a88ce03fdbcf990a8bcb672d579f6a39504765264f37de9b4b1f",
  "audit_machine":
"4b83bafd81b3fe78595ff1e40cfe127760d98d199ec7544a625080d4c9787bf0",
  "result": "PASS",
  "sig": "MEUCIQD1pPVmMRtvvOCAQMR+hzB+e1I62H7HU6dO1QTsuQTglgIg..."
}

```

Key observations:

- `prev` links to SHA-256 of attestation #5 — chain is unbroken
- `fingerprint.machine` and `fingerprint.config` unchanged across all 6 attestations — same machine, same security configuration
- `audit_native` + `audit_machine` — dual audit hashes, both deterministic and independently verifiable
- `sig` — ECDSA P-256 signature, verifiable with agent's registered public key

Machine Audit Detail (Behind `audit_machine` Hash)

```

{
  "ts": "2026-02-09T09:30:09Z",
  "checks": {
    "fs.state_dir_perms": { "status": "ok", "detail": "State dir permissions OK" },
    "fs.config_perms": { "status": "ok", "detail": "Config permissions OK" },
    "fs.credentials_perms": { "status": "ok", "detail": "Credentials dir permissions OK" },
    "fs.syncd_folder": { "status": "ok", "detail": "Not in syncd folder" },
    "fs.suid_sgid": { "status": "ok", "detail": "No SUID/SGID files" },
    "net.listening_ports": { "status": "ok", "detail": "No unexpected listening ports" },
    "fw.macos": { "status": "warn", "detail": "macOS firewall not enabled" },
    "skills.inventory": { "status": "ok", "detail": "4 skills installed" },
    "skills.pattern_scan": { "status": "warn", "detail": "10 suspicious patterns (review needed)" },
    "ops.model_allowlist": { "status": "ok", "detail": "Model allowlist consistent" }
  },
  "summary": { "ok": 8, "warn": 2, "fail": 0 }
}

```

Chain Verification

 ClawdSure Chain Verification

#12026-02-08T07:01:29Z✓signature valid

#22026-02-08T07:01:37Z✓signature valid

#32026-02-08T07:19:37Z✓signature valid

#42026-02-08T07:47:06Z✓signature valid

#52026-02-08T09:30:10Z✓signature valid

#62026-02-09T09:30:09Z✓signature valid

Chain: 6 attestations | 0 errors | 0 warnings

 CHAIN VALID

Anyone with the agent's public key can independently verify every signature and hash link.

Chain Integrity Rules

Condition	Effect
Daily PASS attestation	Chain continues ✓
FAIL (critical findings)	48-hour grace period to remediate
Remediated within grace	Chain continues ✓
No attestation for 48 hours	Chain broken ✗
Chain broken	Coverage void until re-enrollment

Simple. Deterministic. No ambiguity. When an incident occurs, the chain validity at that moment determines claim eligibility — just like a motor telematics black box.

Actuarial Analysis

Industry Benchmarks (2024-2025)

Metric	Value	Source
Global agent security market	\$15B (2024)	Security.org
Market growth rate	30% CAGR	Security.org
Average breach cost	\$4.45M	IBM
SMB breach rate (any incident)	~43% annually	Verizon DBIR
Agent breach insurance loss ratio	45-65%	Industry average
Unreported incidents	91.5%	German BKA

Claim Rate Estimation

Baseline: Uncontrolled SMB population

Incident Type	Annual Rate	Source
Any cyber incident	43%	Verizon DBIR
Data breach	28%	Ponemon
Ransomware	15-20%	Coalition
BEC/fraud	12%	FBI IC3

Controlled: ClawdSure population (with continuous attestation)

Security controls compound to reduce breach probability:

Control	Risk Reduction	Source
Regular patching	60%	CISA
MFA enabled	80-90%	Microsoft
Security audits	50-70%	Various
Continuous monitoring	30-50%	Gartner

Compounded reduction:

Base rate:	30%
× (1 - 0.60) patch compliance	= 12%
× (1 - 0.50) security audit	= 6%
× (1 - 0.30) continuous monitoring	= 4.2%

Estimated claim rate for attesting agents: 3-6%

Core Pricing: \$50 Premium → \$500 Payout

Premium (P):	\$50
Payout (L):	\$500
Target Loss Ratio (LR):	60%
Max Expected Loss:	$P \times LR = \$30$
Max Claim Rate:	$\$30 / \$500 = 6.0\%$
Estimated Claim Rate:	4.2%
Margin of Safety:	30%

Sensitivity Analysis (Underwriting Only)

Claim Rate	Expected Loss	Loss Ratio	Viable?
2%	\$10	20%	✅ Very profitable
4%	\$20	40%	✅ Profitable
6%	\$30	60%	✅ Target
8%	\$40	80%	⚠️ Marginal
10%	\$50	100%	❌ Break-even

Statistical Credibility

Using Bühlmann credibility theory:

```

n = k² / (p × (1-p))
n = 0.05² / (0.05 × 0.95)
n ≈ 385 policies minimum for statistical credibility

```

Unit Economics

Per-Policy (Without Yield)

Component	Amount	% of Premium
Premium	\$50.00	100%
Expected claims (55% LR)	(\$27.50)	55%
Acquisition cost	(\$5.00)	10%
Admin/tech	(\$7.50)	15%
Underwriting profit	\$10.00	20%

The HyperSend Advantage: DeFi Yield on Float

Premiums collected in USDT are routed to Morpho vaults via HyperSend (existing Kryptoplus infrastructure, battle-tested with casino deposit routing). This earns 6-12% APY on premium float.

```

Agent pays $50 USDT
↓
HyperSend Router
↓
Morpho Vaults (6-12% APY, USDT lending markets)
↓
Yield accrues to ClawdSure reserve
↓
Claims paid instantly in USDT

```

Traditional insurers earn 3-5% on float (bonds, equities). ClawdSure earns 6-12% on float (DeFi). This structural advantage compounds at scale.

Yield Per Policy

APY Scenario	Yield/Policy	As % of Premium
6% (conservative)	\$1.50	3.0%
9% (base case)	\$2.25	4.5%
12% (optimistic)	\$3.00	6.0%

Per-Policy (With Yield at 9% APY)

Component	Without Yield	With Yield
Premium	\$50.00	\$50.00
Investment income	\$0.00	\$2.25
Effective revenue	\$50.00	\$52.25
Claims (55% LR)	(\$27.50)	(\$27.50)
Expenses (25%)	(\$12.50)	(\$12.50)
Net margin	\$10.00 (20%)	\$12.25 (24.5%)
Combined ratio	95%	90%

Sensitivity With Yield

Claim Rate	UW Loss	Yield	Net Result	Viable?
4%	\$20	+\$2.25	\$30.25 profit	✅ Excellent
6%	\$30	+\$2.25	\$20.25 profit	✅ Good
8%	\$40	+\$2.25	\$10.25 profit	✅ Marginal → OK
10%	\$50	+\$2.25	\$0.25 profit	⚠️ Break-even
12%	\$60	+\$2.25	(\$9.75) loss	❌ Loss (less severe)

Yield extends viability from ≤6% claim rate to ≤10%.

Loss Distribution

Incident Type	Frequency	Avg Severity	Expected Cost
Credential theft	40% of claims	Low (\$250)	\$7.50/policy
Unauthorized access	30%	Medium (\$500)	\$7.50/policy
Data exfiltration	20%	High (\$500)	\$5.00/policy
Supply chain compromise	10%	Critical (\$500)	\$5.00/policy
Total			\$25.00/policy

Financial Projections (5-Year)

Target Ratios

Component	Target
Loss Ratio	55%
Expense Ratio	25%
Combined Ratio (UW only)	80%
Investment Income	+5-8%
Combined Ratio (with yield)	~85%
ROE at scale	20-25%

Forecast

Year	Policies	GWP	Yield (9%)	Claims (55%)	Expenses (25%)	Net Profit
2026	50K	\$2.5M	\$113K	\$1.38M	\$625K	\$613K
2027	200K	\$10M	\$450K	\$5.5M	\$2.5M	\$2.45M
2028	500K	\$25M	\$1.13M	\$13.75M	\$6.25M	\$6.13M
2029	1M	\$50M	\$2.25M	\$27.5M	\$12.5M	\$12.25M
2030	2M	\$100M	\$4.5M	\$55M	\$25M	\$24.5M

Float at Scale

Policies	GWP	Average Float	Annual Yield (9%)
50K	\$2.5M	\$1.25M	\$113K
500K	\$25M	\$12.5M	\$1.13M
2M	\$100M	\$50M	\$4.5M
5M	\$250M	\$125M	\$11.25M

At 5M policies, **yield alone covers 40% of expected claims.**

Total Addressable Market

Segment	Agents (2028)	Penetration	Premium Potential
OpenClaw ecosystem	2M	25%	\$25M
Enterprise autonomous	3M	15%	\$22.5M
Prosumer/developer	5M	10%	\$25M
Total	10M	15%	\$72.5M

Year 1 target: 50,000 policies = \$2.5M GWP

Year 3 target: 500,000 policies = \$25M GWP

Premium Adjustments & Risk Scoring

Risk-Based Pricing

Factor	Adjustment
Base premium	\$50
+Critical findings history	+30%
+Public-facing gateway	+25%
+Elevated execution enabled	+20%
+Browser tools enabled	+15%
+No relay backup	+10%
–Continuous chain >1 year	–10%
–Zero warnings (90 days)	–5%

Premium range: \$32 - \$85

Risk Scoring

Base Score: 100	
Deductions:	
Critical finding (current):	–50 each
Machine audit failure:	–25 each
Warning (current):	–5 each
Critical remediated (90 days):	–10 each
Chain gap (48h+):	–25 each
Version outdated (>2 minor):	–10

Additions:

Clean audit streak (30+ days):	+10
Clean audit streak (90+ days):	+20
All attestations relayed:	+5

Score	Tier	Effect
90-100	Excellent	Eligible for discounts
70-89	Good	Standard pricing
50-69	Fair	+10% surcharge
<50	Poor	Ineligible / must remediate

Product Tiers

Feature	Basic	Pro	Enterprise
Premium	\$50/year	\$200/year	Custom
Payout	\$500	\$2,500	Custom
Ratio	10:1	12.5:1	Negotiated
Min chain	None	30 days	90 days
Target LR	55%	50%	Negotiated

Covered Incidents & Claim Assessment

Eligible incidents (with valid chain at time of occurrence):

- Verified supply chain compromise affecting insured agent
- Platform vulnerability with CVE affecting insured OpenClaw version
- Configuration tampering detected (config hash change without attestation PASS)
- Unauthorized access verified by attestation chain anomaly

Each incident is assessed like a motor claim:

1. Was the attestation chain valid at the time of incident?
2. Does the incident match covered breach types?
3. Were exclusions present?

Exclusions:

- Chain broken at time of incident (no attestation within 48h)
- Self-inflicted (operator disabled security controls — detectable via config hash drift)
- Pre-existing critical findings at enrollment

- Gross negligence (ignoring critical findings for >48h)
- Social engineering without technical breach

Capital Requirements & Reserve Model

Phase	Policies	Reserve Requirement	Capital Need
Seed	0-5K	\$250K	\$500K
Series A	5K-25K	\$1.25M	\$2.5M
Series B	25K-100K	\$5M	\$10M
Scale	100K+	\$25M+	Reinsurance treaty

Reserve formula: 3× expected annual losses

- At Basic tier: Reserve = 3 × (policies × \$500 × 0.05) = 7.5% of max payout capacity

Reinsurance Proposal

Quota Share Treaty

Parameter	Proposed
Cession	50%
Commission	30%
Loss corridor	50-80% LR
Profit commission	25% of profit

Greenlight Re Projected Returns

Year	Ceded Premium	Ceded Yield	Expected Loss	Commission	Net to GLRe
2026	\$1.25M	\$56K	\$688K	\$375K	\$244K
2027	\$5M	\$225K	\$2.75M	\$1.5M	\$975K
2028	\$12.5M	\$563K	\$6.88M	\$3.75M	\$2.44M
2029	\$25M	\$1.13M	\$13.75M	\$7.5M	\$4.88M
2030	\$50M	\$2.25M	\$27.5M	\$15M	\$9.75M

Catastrophe Protection

Layer	Scope	Est. Premium
Working layer (\$0-\$50K)	Self-retained	—
First excess (\$50K-\$250K)	Quota share 50%	~\$5K/yr
Catastrophe (\$250K+)	Stop-loss / XOL	~\$10K/yr

Covers correlated events (0-day affecting multiple agents simultaneously).

Stress Testing

Scenario	Claim Rate	Loss Ratio	Action
Base case	4.5%	45%	Continue
Moderate stress	8%	80%	Increase premium
Severe stress	12%	120%	Stop writing, reserve
Catastrophe (0-day)	30%	300%	XOL recovery

Expansion Strategy

Phase 1: OpenClaw (2026)

- First mover in viral personal agent ecosystem
- Hardest security problem (personal machines, varied configs)
- Proves the model

Phase 2: Enterprise Agent Frameworks (2027)

- Langchain
- Vercel AI SDK
- AutoGPT / CrewAI
- Adapt attestation scripts per framework

Phase 3: Full Agent Economy (2028+)

- Trading bots
- Home automation agents
- Coding agents (Devin-style)
- Multi-agent systems
- Custom attestation modules per vertical

Why Greenlight Re

1. **Innovation appetite** — track record backing novel risk classes
2. **Tech & security expertise** — already writes tech, aviation, political risk

3. **Data-driven** — our attestation model provides unprecedented risk visibility
 4. **Aligned incentives** — quota share = shared upside
 5. **First mover** — no competing product exists in AI agent breach insurance
 6. **Limited downside** — low individual limits, diversified book
-

About the Team

Mark Musson — Founder, Kryptoplus Labs

- Previously built and sold a dynamic by-the-second motor pricing MGA to AON, reaching £40m GWP
- 6 years building real-time pricing, telematics data pipelines, and insurance product design
- Deep domain expertise in telematics-based pricing and underwriting unit economics

Kryptoplus Labs (krypto.plus) — Infrastructure for the autonomous economy

- **HyperSend**: Battle-tested DeFi yield routing (casino deposit → Morpho vaults)
 - **ClawdSure**: Telematics-based agent breach insurance for AI agents
-

Next Steps

1. **Review this concept note and proof chain**
 2. **Technical deep dive** — walk through attestation system, IPFS pinning, oracle verification
 3. **Actuarial collaboration** — refine trigger events, exclusion matrix, pricing model with attestation chain data
 4. **Capacity discussion** — structure and terms for Greenlight Re participation
-

Contact:

Mark Musson

Founder, Kryptoplus Labs

markmusson@gmail.com

krypto.plus