S E N T I N E L

Shared Environmental Network for Tracking Identified and Nonidentified Entities in Low-altitude

FOUNDING WHITEPAPER | VERSION 1.0

Founded by Damon Scott Mayo
March 20, 2026

Blockchain Verified | Contract: 0x1785c905a3ba84b03ced124d71ce9caa3431bc18
Polygon Mainnet | Block 84440112 | 09:50:57 UTC

1. Executive Summary

SENTINEL is a decentralized, blockchain-anchored network of consumer-grade and home-based radar systems designed to monitor, detect, and permanently record aerial phenomena across the United States and eventually the world. Built on the same principles that power the Helium Network, SENTINEL puts the tools of aerial surveillance directly in the hands of ordinary citizens — removing governments, corporations, and even its own founders from the ability to suppress, alter, or control the data it collects.

The sky above us is increasingly active. Unidentified Aerial Phenomena (UAP) continue to be reported by military pilots, commercial aviators, and civilians at unprecedented rates. Foreign adversarial drones have appeared over sensitive U.S. infrastructure. And yet, the public has no independent, tamper-proof system for monitoring what moves through our shared airspace.

> ***"Not even the founder of SENTINEL will be able to keep this information away from the people. That is the entire point." — Damon Scott Mayo, Founder***

SENTINEL changes this. Every detection is cryptographically timestamped, independently verified by multiple nodes, and stored permanently on a public blockchain that no single authority can alter. The network rewards participants with $SNTL tokens, creating a self-sustaining ecosystem where everyday people are paid to watch the sky — and where the data they generate belongs to everyone.

2. The Problem

2.1 The UAP Data Crisis

Despite decades of sightings reported by credible witnesses — including military personnel, commercial pilots, and law enforcement — the UAP community faces a fundamental and persistent problem: a near-total absence of tamper-proof, scientifically defensible data. The existing evidence landscape is dominated by eyewitness accounts and low-resolution photography that are easily dismissed. Even when government agencies collect radar data related to UAP events, that data is classified, withheld, or quietly discredited.

The result is a credibility gap that has frustrated researchers, stonewalled congressional investigators, and left the public without answers to questions that may have profound implications for national security, science, and our understanding of reality itself.

2.2 The Drone Threat

The UAP monitoring challenge now intersects with an urgent national security concern. Unmanned aerial vehicles — drones — operated by foreign adversaries, criminal organizations, and unknown actors have been documented near military bases, power infrastructure, airports, and populated areas. In late 2024, a wave of mysterious drone sightings over New Jersey and military installations drew congressional attention and demonstrated that the United States lacks a coherent, distributed, civilian-accessible system for tracking low-altitude aerial activity.

Law enforcement agencies are overwhelmed. Existing radar infrastructure is military-controlled, classified, and inaccessible to the public. There is no citizen-facing equivalent of a distributed seismic network for the sky.

2.3 The Trust Problem

Even when aerial anomaly data is collected by government agencies, the public has little reason to trust its completeness or accuracy. Decades of documented suppression, classification, and institutional denial have created a justified skepticism. Any monitoring system controlled by a single organization — government, corporate, or otherwise — is vulnerable to the same pressures that have kept UAP data hidden for generations.

> ***The problem is not a lack of phenomena to observe. The problem is a lack of infrastructure that cannot be silenced.***

3. The Solution: SENTINEL

3.1 What SENTINEL Is

SENTINEL is a decentralized physical infrastructure network (DePIN) that connects thousands of consumer-grade radar sensors operated by ordinary people in their homes, yards, and communities. Each sensor node continuously monitors the airspace above it, processes detection data locally, and submits cryptographically signed records to a public blockchain — creating a

permanent, distributed, tamper-proof log of aerial activity that no single entity can suppress or alter.

3.2 How It Works

The SENTINEL network operates as a three-layer system working in concert:

- Layer 1 — The Sensor Node: A consumer radar module (mmWave technology, 60-77 GHz) housed in a weatherproof enclosure monitors the local airspace. Raw detection data is processed locally by a small embedded computer such as a Raspberry Pi, which filters noise, classifies detections, and generates a cryptographic signature for each event.
- Layer 2 — The Data Pipeline: Signed detection records are hashed and submitted to a decentralized storage network (IPFS/Filecoin), with the cryptographic hash anchored to the SENTINEL smart contract on the Polygon blockchain. Raw data is preserved off-chain while an immutable fingerprint is recorded on-chain — making storage affordable and verification absolute.
- Layer 3 — The Blockchain Record: Every detection event is permanently timestamped on the Polygon blockchain. No administrator, government agency, or even the SENTINEL Foundation itself can alter, delete, or suppress these records once written. The blockchain enforces transparency as a technical reality, not merely a policy promise.

3.3 The Detection Tier System

SENTINEL classifies all detections into four tiers based on their degree of explainability. This system filters known aircraft from genuinely anomalous events and directs research attention and token rewards toward the most significant detections.

Tier	Classification	Description	Reward Multiplier
T1	Fully Identified	Matches ADS-B commercial/private flight data	0.5x
T2	Likely Identified	Consistent with drone, bird, or weather balloon	1x
T3	Anomalous	Speed or maneuver exceeds known aircraft capability	3x
T4	Unresolved	No correlation with any known object or phenomenon	5x

Integration with the OpenSky Network and ADS-B Exchange allows SENTINEL nodes to automatically filter and classify commercial and private air traffic in real time, ensuring that T3 and T4 designations represent genuinely unexplained events.

4. Technology Architecture

4.1 Radar Hardware

SENTINEL is designed around commercially available, FCC Part 15 compliant mmWave radar modules that require no operating license. The primary target hardware is the Texas Instruments IWR6843 series, a 60-64 GHz millimeter wave radar-on-chip that is already used in automotive safety systems, industrial sensing, and smart home devices. Its consumer availability, low cost, and regulatory approval make it ideal for mass deployment.

Specification	Value
Frequency Band	60-64 GHz (FCC Part 15 compliant)
Detection Range	Up to 100 meters (standard), up to 500m (enhanced)
Angular Resolution	15 degrees azimuth
Object Detection	Drones, aircraft, birds, large objects
Weather Operation	All-weather (radar unaffected by fog, rain, dark)
Power Consumption	Under 3 watts
Approximate Cost	$50-150 USD per unit

4.2 Blockchain Infrastructure

SENTINEL operates on the Polygon blockchain — an Ethereum-compatible Layer 2 network chosen for its negligible transaction costs (fractions of a cent per submission), high throughput, and environmental efficiency. The SENTINEL smart contract suite handles device registration and identity, event submission and timestamping, token rewards distribution, and geographic zone management.

Device identity is anchored cryptographically: each node generates a unique keypair at setup, and all submitted data is signed by that key. This makes spoofed or fabricated detections computationally infeasible to inject into the network without detection.

4.3 Data Storage

Raw radar detection data is stored on IPFS (InterPlanetary File System) with long-term persistence provided by Filecoin. Only the cryptographic hash of each detection package is written to the blockchain, keeping on-chain costs minimal while preserving the ability to verify any individual record against its blockchain fingerprint. This architecture makes data both permanently verifiable and practically retrievable.

5. The $SNTL Token and Incentive Design

5.1 Purpose of the $SNTL Token

The $SNTL token is the economic engine of the SENTINEL network. It serves three functions: rewarding node operators for contributing genuine aerial monitoring coverage, incentivizing geographic diversity over concentration, and enabling community governance of the SENTINEL protocol through decentralized voting.

5.2 The Coverage-First Reward Model

Unlike traditional cryptocurrency mining — where buying more hardware directly translates to more income — SENTINEL's reward model is deliberately designed to favor geographic diversity over raw quantity. This design decision is fundamental to SENTINEL's mission: a network that truly monitors the sky needs coverage everywhere, not concentration in a few locations.

> ***A second radar sensor in the same living room produces redundant data the network already has. A sensor in an unmonitored rural county produces information nobody else can provide. SENTINEL rewards what the network actually needs.***

Key mechanisms enforcing this model include:

- Geographic Exclusion Zones: A minimum radius of 500 meters to 1 kilometer within which only one node earns full rewards. Additional nodes within the same zone receive sharply diminished returns, making it economically irrational for large operators to saturate any single area.
- Data Novelty Scoring: Nodes are rewarded not merely for uptime but for contributing detection data that differs meaningfully from what nearby nodes are already seeing. A

node in an underserved area earns more because its data adds more value to the network.

- Detection Tier Multipliers: T3 and T4 anomalous detections generate significantly higher rewards than routine T1 and T2 classifications, incentivizing nodes in areas of genuine aerial interest.
- Diminishing Returns Per Identity: Reward multipliers are capped per registered identity, adding friction to large-scale farming operations without penalizing legitimate multi-location operators.

5.3 Why This Matters for Small Participants

The coverage-first model means that a homeowner who installs a single SENTINEL node in an unmonitored area earns competitive rewards relative to a well-funded operator running dozens of devices in a saturated city. Scaling beyond a handful of devices requires real-world access to genuinely distinct locations — a cost and logistical challenge that naturally limits the advantage of large-scale operators and keeps the network economically accessible to everyday participants.

6. SENTINEL as Citizen Science

6.1 Democratizing Aerial Observation

Throughout history, some of the most significant scientific discoveries have been made not by institutions but by passionate individuals with access to the right tools. SENTINEL extends this tradition to aerial monitoring — giving anyone with a home, a window, and a desire to contribute the ability to participate in one of the most important observational networks ever assembled.

The scientific value of distributed citizen sensing networks is well established. Projects like SETI@home, the Community Collaborative Rain, Hail and Snow Network (CoCoRaHS), and the American Meteor Society have demonstrated that coordinated citizen observation can produce data of genuine scientific merit. SENTINEL applies this model to the most compelling and least-monitored domain of citizen science: our own airspace.

6.2 Open Data for Open Science

All SENTINEL detection data — with the exception of personally identifying node location information, which participants may choose to keep private — is publicly accessible. Researchers, universities, government agencies, and independent investigators can access the full SENTINEL

dataset through a public API, enabling independent analysis, peer review, and scientific publication.

This openness is enforced not by policy but by architecture. Because the data lives on a public blockchain and a decentralized storage network, no organization — including the SENTINEL Foundation — has the technical ability to restrict access to it. The data belongs to the network, and the network belongs to everyone.

7. National Security Implications

7.1 The Drone Monitoring Gap

The emergence of small, commercially available unmanned aerial vehicles as tools of surveillance, disruption, and potential attack represents one of the most significant security challenges of the current decade. Military and law enforcement radar infrastructure is not designed for the distributed, low-altitude monitoring that effective drone detection requires — and it is not accessible to the public that often first observes these incursions.

SENTINEL fills this gap. A nationwide network of ground-level radar sensors, each continuously monitoring its immediate airspace and logging detections to an immutable public record, creates exactly the kind of distributed early warning infrastructure that neither the military nor law enforcement currently possesses in a public-facing form.

7.2 Complementing Official Infrastructure

SENTINEL is explicitly designed as a complement to, not a replacement for, official aerial monitoring systems. The network does not interfere with any aircraft or aerial system. It does not jam signals or transmit in controlled spectrum. It listens, records, and reports — functions that are entirely legal, entirely peaceful, and entirely compatible with existing regulatory frameworks.

SENTINEL detection data, particularly corroborated multi-node events, could serve as a valuable resource for congressional oversight committees, the FAA's UAP reporting office, and academic researchers studying aerial phenomena. The network's immutable, timestamped records provide exactly the kind of evidence base that official investigations have historically lacked.

> ***When multiple SENTINEL nodes in a geographic region simultaneously***

> ***detect an anomalous aerial object, that corroborated event is automatically flagged, archived, and made permanently available to any researcher, journalist, or official who wishes to examine it. No one can make it disappear.***

8. Challenges and Obstacles

SENTINEL is an ambitious project and intellectual honesty requires acknowledging the significant challenges ahead. The founding team is committed to transparency about these obstacles as a matter of scientific integrity and community trust.

Challenge	Description	Mitigation Strategy
Hardware Cost	Initial node hardware costs ~$150, limiting early adoption	Crowdfunding, grant funding, and hardware partner negotiations to reduce costs
False Positive Rate	Consumer radar may generate significant non-anomalous detections	T1/T2 auto-filtering via ADS-B integration and machine learning classification
Geographic Coverage	Meaningful coverage requires thousands of nodes across diverse regions	Token incentives designed specifically to reward underserved geographic areas
Regulatory Navigation	FAA and FCC rules must be carefully observed	Legal counsel retained; network designed as passive detection only
Data Quality	Node operators may have varying technical capabilities	Simplified setup process; automated data validation; community support
Funding	Significant capital required for development and infrastructure	Dual nonprofit/LLC structure; grant applications; community crowdfunding
Credibility	UAP topic carries stigma in some scientific communities	Rigorous data standards; academic partnerships; focus on drone detection as entry point

9. Why Now

The convergence of several distinct trends makes 2026 the ideal moment to launch SENTINEL:

- Congressional UAP Momentum: The UAP Disclosure Act, the All-domain Anomaly Resolution Office (AARO), and multiple congressional hearings have created unprecedented official acknowledgment of the UAP phenomenon. Public appetite for credible, independent data has never been higher.

- Available Technology: The mmWave radar modules that power SENTINEL cost less than $150 today. Five years ago, comparable technology cost tens of thousands of dollars. Consumer-grade radar capable of meaningful aerial detection is now genuinely accessible to everyday people.
- Blockchain Maturity: The infrastructure required to run a decentralized physical network — low-cost blockchains, decentralized storage, token distribution systems — is mature, battle-tested, and available. The Helium Network proved this model works at scale.
- Drone Proliferation: The rapid growth of commercial and adversarial drone activity has created a mainstream, non-stigmatized entry point for SENTINEL's monitoring capabilities, broadening the potential user and supporter base far beyond the traditional UAP community.
- Community Readiness: The citizen science and UAP research communities are organized, passionate, and looking for a credible, participatory project to support. SENTINEL gives them one.

10. Development Roadmap

Phase	Timeline	Key Milestones
Phase 1: Foundation	Now - Month 3	Whitepaper publication, legal entities formed, domain & social media secured, provisional patent filed, community launched
Phase 2: Prototype	Month 3 - Month 9	Working single-node prototype, testnet smart contract deployed, first grant applications submitted, 100+ community members
Phase 3: Pilot Network	Month 9 - Month 18	10-node pilot network, ADS-B integration live, academic partnerships established, $SNTL tokenomics finalized
Phase 4: Public Launch	Month 18 - Month 36	Mainnet launch, open hardware certification, public data API, 1,000+ active nodes, congressional briefings
Phase 5: Scale	Year 3+	10,000+ nodes nationwide, international expansion, peer-reviewed publications, established research partnerships

11. Organizational Structure

11.1 Dual Entity Model

SENTINEL operates through two complementary legal entities designed to maximize both public trust and long-term sustainability:

- SENTINEL Foundation Inc. (Florida Nonprofit 501c3): The Foundation owns the SENTINEL mission. It conducts and funds research, builds the community, establishes academic partnerships, accepts tax-deductible donations, and applies for scientific grants. The Foundation employs the founding team and ensures SENTINEL's public interest mission is legally protected in perpetuity.
- SENTINEL Technologies LLC (Florida For-Profit): The LLC holds the intellectual property portfolio including patents, the $SNTL token, hardware certification standards, and commercial licensing rights. Revenue from IP licensing, hardware certification, and data products flows through the LLC, providing long-term financial sustainability for the project and its founders.

11.2 Governance

The SENTINEL Foundation is governed by a Board of Directors committed to the organization's public interest mission. As the network matures, governance of the SENTINEL protocol will progressively transition to a decentralized autonomous organization (DAO) structure in which $SNTL token holders participate in key network decisions — ensuring that control of SENTINEL ultimately rests with its community of participants.

12. How to Get Involved

12.1 For Potential Co-Founders

SENTINEL is actively seeking founding team members who share the conviction that the sky belongs to everyone. We are looking for individuals with backgrounds in electrical engineering and radar systems, blockchain and smart contract development, nonprofit management and grant writing, scientific research and data analysis, and community building and communications. If you believe in radical transparency, citizen empowerment, and the importance of what may be the defining scientific question of our era, we want to hear from you.

12.2 For Node Operators

You do not need a technical background to participate in SENTINEL. If you have a home, a yard, or access to any outdoor location, you can become a SENTINEL node operator. Hardware setup will be designed to be as simple as plugging in a device and connecting to an app. Early node operators will receive founding member status and enhanced token rewards in recognition of their role in building the network from the ground up.

12.3 For Researchers and Institutions

SENTINEL welcomes partnerships with universities, research institutions, and independent scientists. The SENTINEL Foundation will provide research partners with priority access to corroborated event data, technical documentation, and collaborative publication opportunities. Academic credibility is essential to SENTINEL's mission and we are committed to supporting rigorous independent analysis of our data.

12.4 For Donors and Grant Makers

The SENTINEL Foundation is a Florida nonprofit corporation pursuing 501c3 tax-exempt status. Donations to the Foundation will be tax-deductible upon approval of exempt status. We are actively seeking grant funding from scientific research foundations, UAP-focused philanthropists, and public interest technology funders. The Sol Foundation, NASA Citizen Science programs, and NSF Public Participation in STEM grants are among our initial targets.

13. Founding Record and Intellectual Property

The SENTINEL concept was originated by Damon Scott Mayo on March 20, 2026. The founding of this project is permanently recorded on the Polygon blockchain and is publicly verifiable by anyone. This record cannot be altered, deleted, or disputed.

Record Field	Value
Founder	Damon Scott Mayo
Project Name	SENTINEL
Contract Address	0x1785c905a3ba84b03ced124d71ce9caa3431bc18
Transaction Hash	0x2e20d71badb4dad02915232c76dc3d0c76e9637faa9a8430dfea0a50dfc140fe
Document SHA256 Hash	b23824832847129 03b8bc695c0570dd012e87e12efa1efb45cd36f79bd5e43ef
Timestamp	2026-03-20 09:50:57 UTC
Blockchain Network	Polygon Mainnet
Block Number	84440112
Verification URL	polygonscan.com/address/0x1785c905a3ba84b03ced124d71ce9caa3431bc18

> ***This whitepaper and all SENTINEL concepts described herein are the intellectual property of Damon Scott Mayo and the SENTINEL Foundation. The blockchain record above constitutes irrefutable prior art establishing the date of conception. Patent applications are pending.***

A Final Word

We live in a moment when the questions humanity has asked about the sky for generations are finally being taken seriously by governments, scientists, and the public. At the same moment, new threats move through our airspace in ways our existing infrastructure cannot track.

SENTINEL is our answer to both. It is a network built on the conviction that the sky belongs to everyone — that the data gathered by watching it should be owned by no one and available to all — and that ordinary people, given the right tools and the right incentives, can build something that no government, no corporation, and no special interest can control or suppress.

> ***The sky has always had witnesses. SENTINEL gives them a voice that cannot be silenced.***

— Damon Scott Mayo, Founder, SENTINEL
March 20, 2026