# Nexara

## Decentralized Dual-Intelligence Subnet for Bittensor

*Combining Real-World Asset Financial Intelligence*
*with Smart Contract Defect Density Prediction*

February 2026 | CONFIDENTIAL — FOR INVESTOR & ACCELERATOR REVIEW

| $500T+ | $200B+ | 0 | Now |
|---|---|---|---|
| Global RWA market being tokenized | Smart contract TVL needing security scoring | Existing decentralized combined competitors | Optimal launch window before market matures |

# Table of Contents

# Executive Summary

Nexara is a Bittensor subnet that solves a problem no one has solved yet: producing a single, verifiable, decentralized intelligence score that combines the financial health of a tokenized real-world asset with the security quality of the smart contract powering it.

Today, DeFi protocols assess these two risks separately — if they assess them at all. Financial risk is handled by centralized providers like Moody's and Bloomberg. Smart contract security is handled by expensive one-time audits from firms like Certik and Trail of Bits. Neither is decentralized. Neither is continuous. And neither combines both signals into one actionable score.

Nexara fixes this by creating a competitive marketplace on Bittensor where AI models (miners) race to produce the most accurate combined intelligence, validators verify accuracy against real-world outcomes, and TAO emission rewards flow to whoever performs best. The result is infrastructure that continuously improves, costs a fraction of centralized alternatives, and is available to any DeFi protocol on earth.

## The Opportunity in One Sentence

Nexara is Bloomberg Terminal plus CertiK Security Audit — decentralized, continuously improving, and accessible to anyone — built on Bittensor's proven incentive infrastructure.

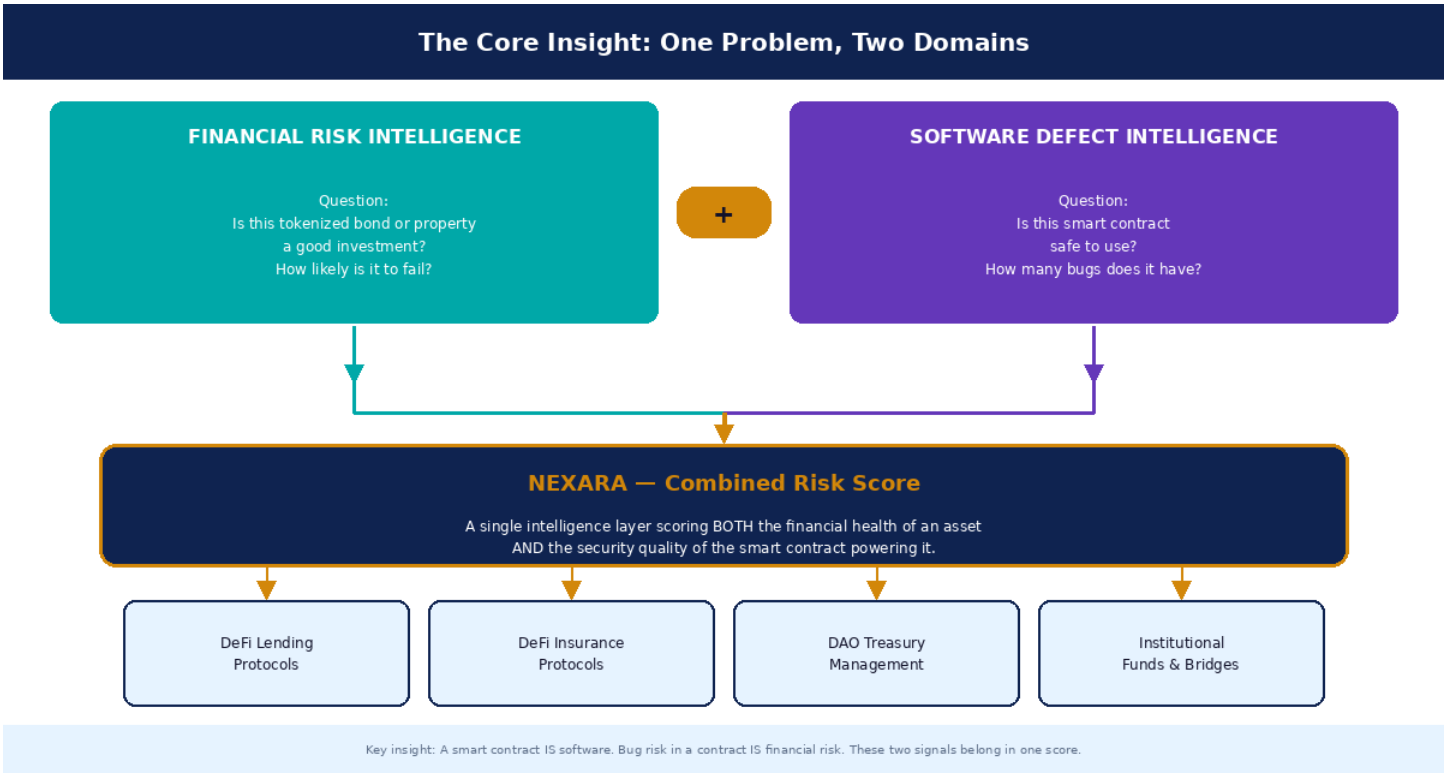
## What Makes This Different From Existing Solutions

| Capability | Bloomberg / Moody's | CertiK / Trail of Bits | Nexara |
|---|---|---|---|
| **Financial Risk Scoring** | Yes — centralized | No | **Yes — decentralized** |
| **Smart Contract Security** | No | Yes — centralized | **Yes — decentralized** |
| **Combined Single Score** | No | No | **Yes — ONLY Nexara** |
| **Continuous Monitoring** | Partial | No (one-time audits) | **Yes — every block** |
| **Outcome-Verified Accuracy** | No | No | **Yes — on-chain proof** |
| **Cost Structure** | $24,000+/year | $50,000+ per audit | **Market rate via TAO** |
| **Open to Anyone** | No — institutional only | No — enterprise only | **Yes — permissionless** |

## The Funding Ask

We are seeking seed investment and accelerator partnership to fund the initial subnet deployment, validator infrastructure setup, miner recruitment, and 12-month operational runway. Full details are in the Tokenomics and Funding Ask section. The goal is to achieve product-market fit — defined as 5+ live DeFi protocol integrations using Nexara intelligence — within 12 months of launch.

# The Core Innovation — Why Combine These Two Ideas?




## Starting Point: Two Powerful but Separate Ideas

ChainAlpha was designed as a decentralized financial intelligence network — AI models competing to price tokenized assets, score their credit risk, and predict their yield. It was inspired by looking at the RWA tokenization boom and asking: who provides the analytical intelligence layer for all these new on-chain assets?

Separately, software defect density prediction is a well-established field in software engineering. Using AI and historical code metrics, researchers have achieved strong accuracy in predicting how many bugs a software module will contain before it is fully tested. This has obvious value for software quality assurance — prioritize testing where bugs are most likely.

## The Insight That Connects Them

> Smart contracts ARE software. Every DeFi protocol — every lending pool, every yield aggregator, every bridge, every tokenized asset vault — runs on smart contract code. That code has bugs. Those bugs get exploited. Exploits destroy value.

> The Ronin bridge lost $625 million. The Poly Network lost $611 million. Nomad lost $190 million. Wormhole lost $326 million. These were not market failures. They were software quality failures. And every single one of them was a financial loss first.
>
> Defect density in a smart contract is not just a software engineering concern. It is a direct measure of financial risk for any asset, protocol, or fund that depends on that contract.

## What the Combination Creates

When you merge financial intelligence with smart contract quality intelligence, you get something qualitatively better than either alone:

- A tokenized bond's true risk score includes not just its credit fundamentals, but also whether the smart contract holding it is secure.
- A DeFi lending protocol's risk score includes not just its collateral quality, but also whether the protocol contract itself could be exploited.
- A yield aggregator's return estimate includes not just market yield factors, but also the probability that a smart contract bug could cause a total loss event.
- An insurance premium for a DeFi position can be priced accurately because both risk dimensions are quantified.

This is why Nexara is not just ChainAlpha plus a bug scanner. It is a fundamentally new class of risk intelligence that did not exist before, because no one had systematically connected these two signals.

# The Problem We Are Solving

## Problem 1 — Financial Intelligence Is Centralized and Expensive

The RWA tokenization market has grown explosively. Tokenized US Treasuries, corporate bonds, real estate, and commodity-backed instruments are now available on-chain across Ethereum, Avalanche, Solana, and dozens of purpose-built chains. But the intelligence layer — the analysis that tells you whether a tokenized asset is worth buying, how risky it is, and what return to expect — is still controlled by traditional institutions.

Bloomberg Terminal charges $24,000 per user per year, calibrated for institutional budgets. Moody's ratings are paid for by the issuers of the assets themselves — creating a direct conflict of interest that was famously catastrophic during the 2008 financial crisis. S&P and Fitch follow the same model. None of these providers were built for on-chain assets, 24/7 markets, or permissionless access.

The result: retail DeFi users, small protocols, and DAO treasuries make financial decisions about tokenized assets with no professional-grade analytical support. They rely on gut feel, social media sentiment, or simply hope.

## Problem 2 — Smart Contract Security Is Reactive, Not Predictive

Security audits are the current standard for smart contract safety. A protocol hires a firm like CertiK or Trail of Bits, pays $20,000 to $200,000 for a manual audit, receives a report, and marks the contract as 'audited.' This audit is done once, at a point in time, and does not update as the codebase evolves.

This model has three fatal flaws. First, audits are reactive — they happen after code is written, not during development. Second, they are static — a contract can pass audit today and have a vulnerability introduced by an upgrade tomorrow. Third, they are binary — a contract is either 'audited' or 'not audited,' with no continuous quality score that investors and protocols can act on.

The numbers tell the story: in 2024 alone, smart contract exploits drained over $2 billion from DeFi protocols. The majority of these protocols had been audited. Audits are necessary but clearly not sufficient.

## Problem 3 — These Two Risk Signals Are Never Combined

Even for well-resourced institutional participants who can afford Bloomberg and also commission audits, the two risk signals live in completely separate silos. There is no single score, no unified intelligence layer, no way to say 'this RWA position has an overall risk-adjusted score of 73 out of 100, accounting for both the financial fundamentals of the underlying asset and the security quality of the smart contract holding it.'

This gap is not a minor inconvenience. It is a structural barrier preventing institutional capital from flowing safely into DeFi. Pension funds, endowments, and family offices that might deploy billions

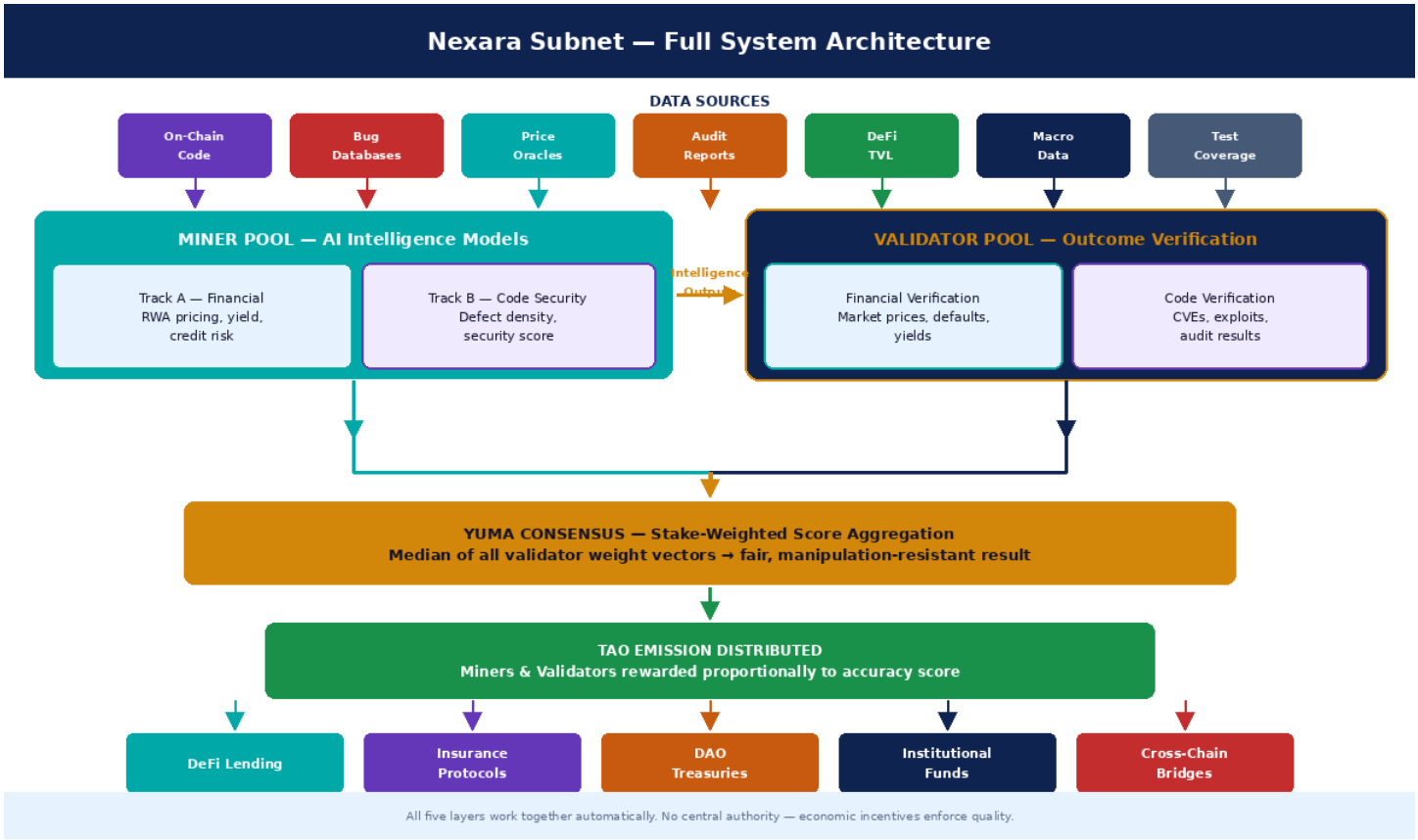
into tokenized assets cannot do so without the kind of comprehensive risk intelligence they take for granted in traditional finance. Nexara builds that intelligence layer.

# How Nexara Works — Visual Architecture

The following charts give a complete picture of the Nexara system. Read them in order — each one adds a layer of detail to the one before it.

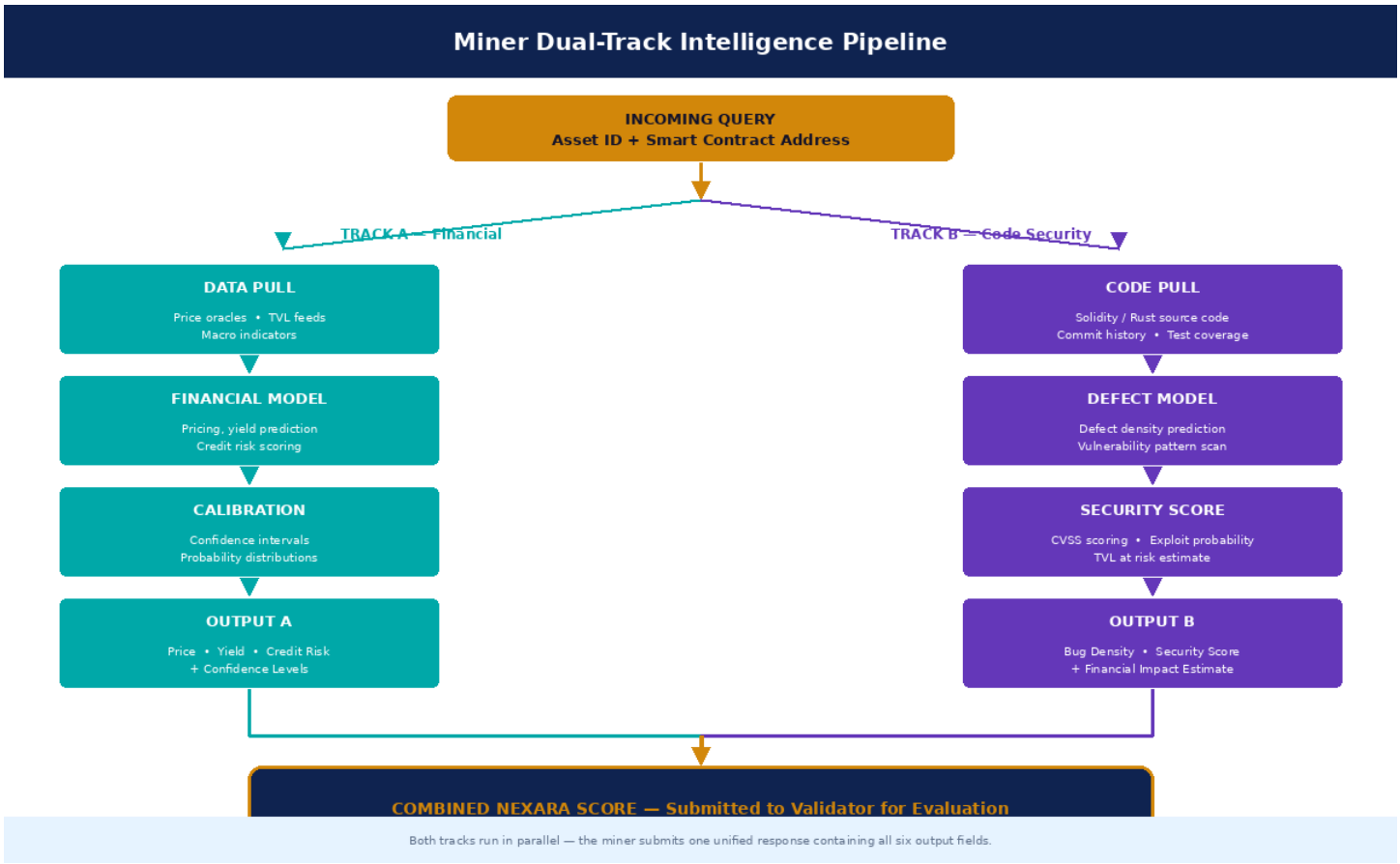
## Chart 1 — Full System Architecture

This shows all five layers of Nexara: data sources, miners (both tracks), validators (both tracks), Yuma Consensus, and end-user consumers.



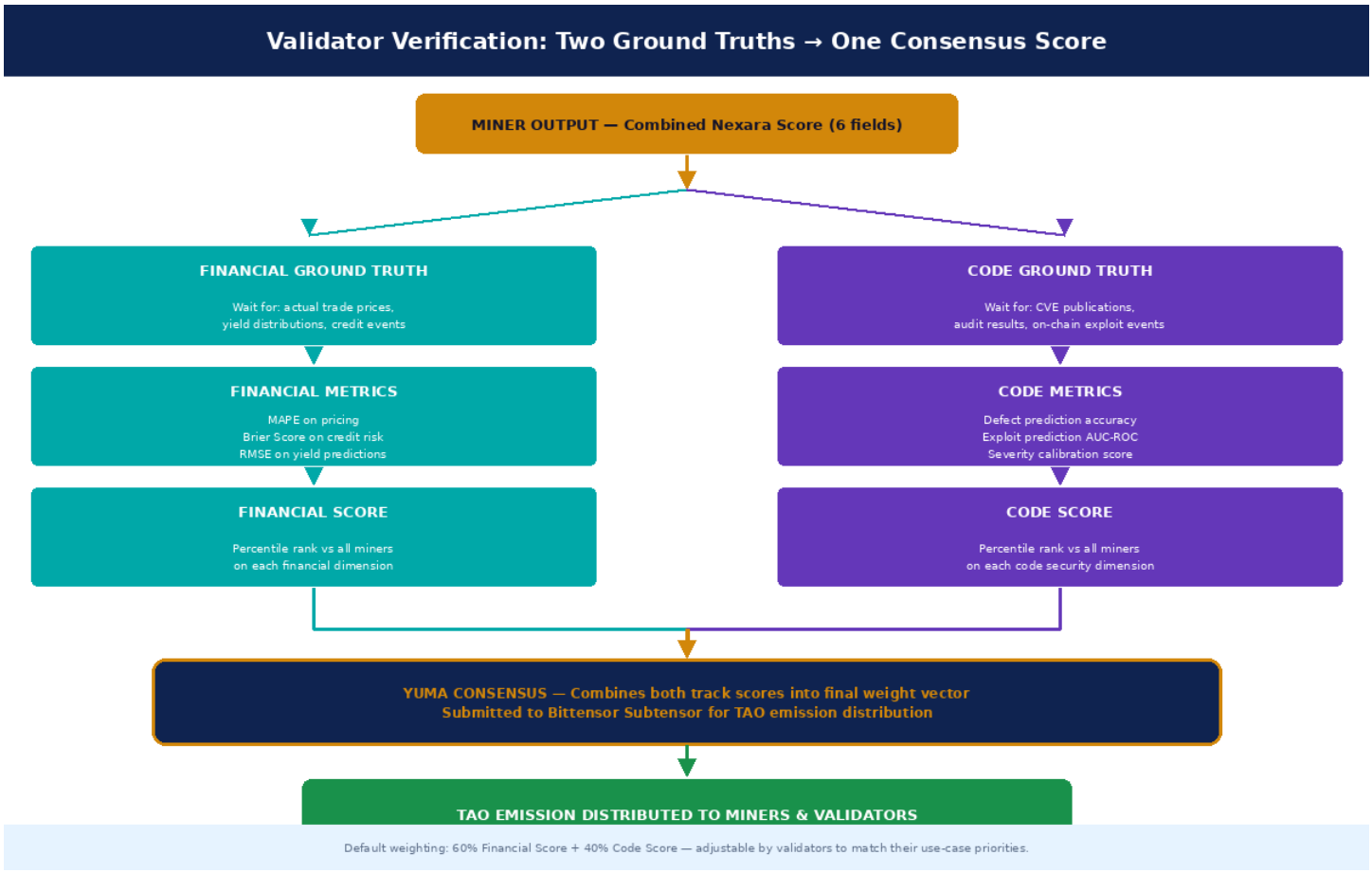

## Chart 2 — The Miner Dual-Track Pipeline

Each miner runs two intelligence pipelines in parallel — one for financial analysis (Track A) and one for smart contract code analysis (Track B). Both outputs are merged into a single Nexara Score before submission to validators.


Miner Dual-Track Intelligence Pipeline
INCOMING QUERY
Asset ID + Smart Contract Address
TRACK A — Financial
TRACK B — Code Security
DATA PULL
Price oracles • TVL feeds
Macro indicators
FINANCIAL MODEL
Pricing, yield prediction
Credit risk scoring
CALIBRATION
Confidence intervals
Probability distributions
OUTPUT A
Price • Yield • Credit Risk
+ Confidence Levels
CODE PULL
Solidity / Rust source code
Commit history • Test coverage
DEFECT MODEL
Defect density prediction
Vulnerability pattern scan
SECURITY SCORE
CVSS scoring • Exploit probability
TVL at risk estimate
OUTPUT B
Bug Density • Security Score
+ Financial Impact Estimate
COMBINED NEXARA SCORE — Submitted to Validator for Evaluation
Both tracks run in parallel — the miner submits one unified response containing all six output fields.

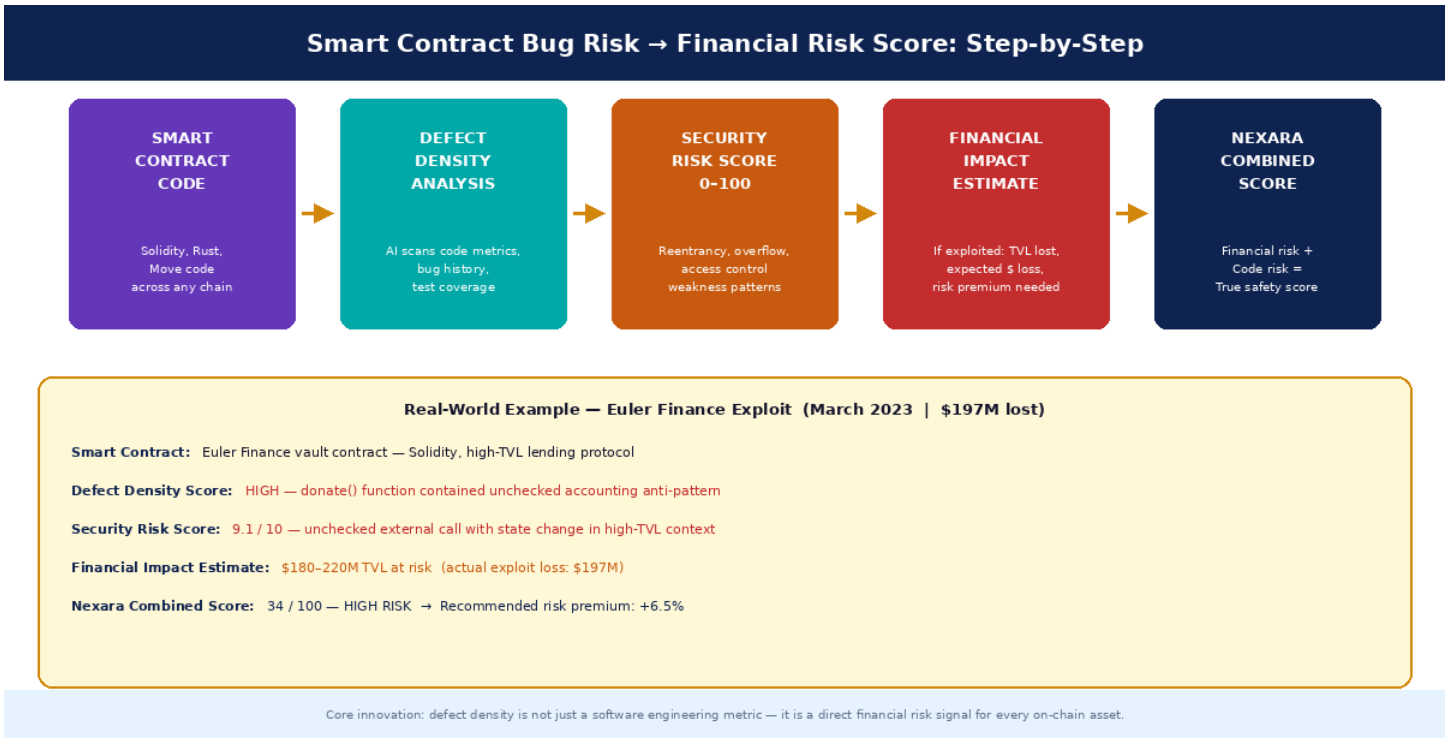
## Chart 3 — Validator Verification with Two Ground Truths

Validators verify miner outputs against two independent ground truths — real market outcomes for financial predictions, and real-world exploit/CVE data for code predictions. Both are then merged into the final consensus weight submitted to the Bittensor protocol.



# Smart Contract Risk → Financial Risk: The Critical Connection

This is the intellectual core of Nexara. Understanding exactly how software defect prediction translates into financial risk scoring is essential for investors, miners, and validators alike.




## Step 1 — Defect Density Prediction on Smart Contract Code

Defect density prediction is a mature field in software engineering. It uses static code analysis metrics — cyclomatic complexity, code churn, coupling between modules, comment density, lines of code per function, and historical bug rates for similar codebases — to predict how many bugs a piece of software is likely to contain per thousand lines of code.

Applied to smart contracts, this technique has been shown in academic research to achieve strong predictive accuracy. The most effective models combine static metrics with dynamic analysis (tracing execution paths) and semantic analysis (understanding what the code is trying to do vs. what it actually does). Nexara miners are incentivized to develop the best possible versions of these models through continuous competitive pressure.

## Step 2 — Translating Bug Density Into Security Risk Score

Not all bugs are created equal. A cosmetic UI bug in a web app has zero financial impact. A reentrancy vulnerability in a smart contract holding $500 million can cause total loss. Nexara miners therefore need to do more than predict how many bugs exist — they need to predict the severity and exploitability of those bugs.

The security risk scoring pipeline applies CVSS (Common Vulnerability Scoring System) methodology, adapted for smart contracts. This scores vulnerabilities on a 0-10 scale based on four factors: attack vector (how easy is the contract to reach?), attack complexity (how hard is exploitation?), privileges required (does the attacker need special access?), and impact (what percentage of TVL could be drained?).

## Step 3 — Translating Security Risk Into Financial Impact Estimate

A security risk score of 8.5 out of 10 means different things for a contract holding $100,000 vs. a contract holding $2 billion. Nexara miners complete the translation by estimating the expected financial loss from exploitation: Security Risk Score × TVL at Risk × Time Exposure Factor = Financial Loss Estimate.

This financial loss estimate is then incorporated directly into the overall Nexara Score for the asset. A tokenized bond held in a highly secure contract might deserve its full credit quality score. The same bond held in a contract with a high-severity vulnerability should have a risk premium added that reflects the probability of total loss from exploitation, regardless of the bond's own credit quality.

## The Historical Validation Case

> Consider the Euler Finance exploit of March 2023, where $197 million was drained via a flash loan attack on a known vulnerable pattern in the donate() function. A Nexara-style analysis of the Euler Finance contract prior to the exploit would have flagged:
>
> • Defect Density Score: HIGH — the vulnerable donation accounting pattern is a known anti-pattern in DeFi code. • Security Risk Score: 9.1/10 — unchecked external calls with state changes in a high-TVL context. • Financial Impact Estimate: $180-220M at risk (close to actual $197M drained). • Recommended Risk Premium for any RWA collateral using this protocol: +6.5%
>
> This pre-exploit intelligence would have let lenders price risk correctly, DeFi insurance protocols set accurate premiums, and institutional funds avoid the position entirely — saving hundreds of millions.

# Incentive and Mechanism Design

Nexara inherits the proven incentive architecture of Bittensor's subnet model and extends it for dual-track intelligence evaluation. The fundamental design principle is unchanged: quality produces rewards, poor quality produces nothing, and the system enforces this automatically without any central authority.

## Dual-Track Emission Mechanics

Every Bittensor block releases a fixed quantity of TAO. Nexara's share of that emission is distributed to participating miners and validators based on a composite quality score derived from both intelligence tracks. Here is the complete flow:

1. A validator selects an evaluation target: a tokenized asset (e.g., a tokenized corporate bond) paired with the smart contract address of the vault or protocol holding it.
2. The validator dispatches the query to all registered miners: 'Produce a complete Nexara Score for this asset and contract pair.'
3. Each miner's dual-track pipeline runs: Track A analyzes the financial fundamentals of the tokenized asset; Track B analyzes the smart contract code quality and security posture.
4. The miner submits a structured response containing six outputs: predicted price, yield estimate, credit risk score (Track A), plus defect density estimate, security risk score, and financial impact estimate (Track B).
5. The validator logs the response. Verification proceeds on two timelines: financial outcome verification waits for market data (hours to months depending on prediction horizon); code outcome verification waits for CVE publications, audit results, and on-chain exploit events.
6. Once verification data arrives, the validator computes dimension scores for each track using objective metrics.
7. Track A scores (MAPE, Brier Score, RMSE, coverage) and Track B scores (defect prediction accuracy, security score calibration, exploit prediction AUC-ROC) are each normalized to percentile rankings.
8. The composite Nexara Score is computed as a weighted combination of Track A and Track B rankings. Default validator weighting: 60% financial + 40% code. Validators may adjust this weighting.
9. Weight vectors from all validators are aggregated through Yuma Consensus (stake-weighted median).
10. TAO emission is distributed proportionally to consensus weights.

## The Eight Evaluation Dimensions

| Track | Dimension | What Is Measured | Verification Method |
|---|---|---|---|
| A | **Pricing Accuracy** | How closely predicted prices match realized market transactions | MAPE vs. on-chain DEX trade data |
| A | **Credit Risk Validity** | Whether risk scores predicted actual credit events (defaults, impairments) | Brier Score + AUC-ROC on realized credit events |

| | | | |
|---|---|---|---|
| **A** | **Yield Prediction** | Accuracy of projected yield vs. realized distribution over the horizon | RMSE against realized yield from protocol data |
| **B** | **Defect Density Accuracy** | Whether predicted bug density matched actual bugs discovered post-deployment | Comparison against CVE disclosures and bug bounty reports |
| **B** | **Security Score Calibration** | Whether high-risk scores correctly identified contracts that were later exploited | AUC-ROC on exploit event ground truth from on-chain data |
| **B** | **Financial Impact Accuracy** | Whether estimated TVL at risk matched actual losses in exploit events | MAPE vs. realized exploit loss amounts from blockchain data |
| **A+B** | **Coverage Breadth** | Proportion of queried asset/contract pairs for which the miner returns valid outputs | Valid response rate across all sampled asset classes and chains |
| **A+B** | **Response Latency** | Speed of response to evaluation queries within timeout window | Millisecond measurement with hard timeout enforcement |

# Economic Alignment for Miners

## The Improvement Flywheel

Miners face a dual-dimension competitive landscape. They cannot simply be good at financial modeling (Track A) and ignore code analysis (Track B) — or vice versa. The composite scoring system means a miner that excels on one track but underperforms on the other will be beaten by a miner with balanced competence across both. This creates incentives for miners to build genuinely integrated intelligence, not siloed expertise.

## Specialization Is Still Rewarded

While composite scoring requires competence in both tracks, miners can still differentiate through specialization in asset class coverage, chain coverage, or depth of code analysis. A miner that develops superior static analysis tooling for Rust-based smart contracts (used on Solana and Near) will outperform on Track B for those chains, driving up their overall composite score. This specialization dynamic produces a rich competitive ecosystem rather than commodity uniformity.

## The Data Infrastructure Arms Race

The primary competitive moat for top miners is data infrastructure. Track A miners need premium financial data subscriptions. Track B miners need access to large code quality training datasets, CVE databases, exploit repositories (such as the Rekt Network database), and smart contract audit reports. Miners who build superior data pipelines will maintain structural accuracy advantages that are difficult for new entrants to replicate quickly. This creates sustainable competitive positions and long-term investment incentives.

# Economic Alignment for Validators

Validators are the integrity layer of Nexara. Their job is to accurately measure miner quality, and the economic system is carefully designed to make honest, careful evaluation the most profitable strategy.

Validators stake TAO to participate. Dishonest or inaccurate evaluations result in their weight vectors being clipped by Yuma Consensus, reducing their influence and therefore their TAO rewards. Validators also compete in the delegation market: TAO holders can move their delegated stake to validators who produce more accurate evaluations, creating a reputation market that rewards evaluation quality over time.

The dual-track verification requirement means validators need to maintain two separate verification infrastructure stacks: financial outcome verification pipelines (oracle networks, DEX data, credit event databases) and code outcome verification pipelines (CVE feeds, exploit event monitoring, audit report databases). This infrastructure investment creates meaningful barriers to entry that ensure only capable operators become validators.

## Failure Modes and Mitigations

| Attack / Failure | How It Could Happen | How Nexara Stops It |
|---|---|---|
| **Historical Code Overfitting** | Miners train on known CVEs to score well on past vulnerabilities but miss novel attack patterns | Evaluation includes newly deployed contracts (under 30 days) with no published CVE history |
| **Exploit Event Manipulation** | Attacker deliberately exploits a low-TVL contract to make miners with good defect scores look bad | Exploit events below $100K TVL threshold excluded from scoring. Multi-oracle exploit confirmation required |
| **Track A / Track B Gaming** | Miners invest heavily in one track and submit random outputs for the other to save compute cost | Composite score formula requires minimum threshold performance on each track independently — random outputs produce zero credit on that dimension |
| **Validator Financial Collusion** | Validators collude to favor miners who pay them kickbacks | Yuma median aggregation — majority must collude to move consensus. Clipping makes deviating validators visible and costly |
| **Copycat Miners** | Multiple miners share a model, reducing competitive diversity while each draws emission | Output fingerprinting detects identical responses. Identical outputs treated as a single miner for scoring purposes |
| **Oracle Source Failure** | A price oracle or CVE feed goes down, making verification impossible for that cycle | Multi-source oracle consensus required. Evaluation cycles with insufficient source confirmation are deferred, not cancelled |
| **Dormant Validator Gaming** | Validator stops submitting weights but retains permit, blocking active operators from joining | Permit decay: influence reduced progressively after 3 missed cycles. Full permit revocation after 14 days of inactivity |

# Miner Design — Building a Dual-Track Intelligence Model

This section is the practical guide for anyone who wants to mine on Nexara. It covers the technical requirements for both tracks, the data infrastructure you will need, how registration works, and what it takes to be competitive.

## What a Nexara Miner Actually Does

A Nexara miner is a server that runs two AI pipelines simultaneously and responds to incoming queries with a structured six-field output: predicted price, yield estimate, and credit risk score (Track A); plus defect density estimate, security risk score, and financial impact estimate (Track B). The quality of these outputs — measured against real market outcomes and real exploit events — determines how much TAO the miner earns.

## Track A — Financial Intelligence Pipeline

### Data Requirements

Track A requires connections to: on-chain token registries for asset metadata, price oracle networks (Chainlink, Pyth, Band Protocol) for historical and current pricing, DeFi protocol TVL data for liquidity context, traditional financial data feeds for comparable instrument benchmarking, and macroeconomic indicator feeds for interest-rate-sensitive assets.

### Model Architecture

Effective Track A models typically combine multiple modeling approaches rather than relying on a single technique. Time series models (LSTM, Transformer-based) handle price prediction. Gradient boosting ensembles handle credit risk classification — they perform well on structured financial data with mixed feature types. Calibrated probability outputs are essential: the Brier Score evaluation metric rewards models that express well-calibrated confidence, not just accurate point predictions.

## Track B — Smart Contract Intelligence Pipeline

### Data Requirements

Track B requires: access to smart contract source code (from Etherscan, Sourcify, and chain-specific explorers), historical CVE and exploit databases (National Vulnerability Database, Rekt Network database, DeFi Hack Analysis repositories), smart contract audit reports (publicly available from CertiK, Trail of Bits, OpenZeppelin), bug bounty program disclosures, and test coverage reports from protocol repositories.

### Model Architecture

Track B models draw on three complementary analysis approaches. Static analysis extracts code metrics: cyclomatic complexity, fan-in/fan-out coupling, halstead complexity measures, function length distribution, external call patterns, and use of known anti-patterns (reentrancy, integer overflow, unchecked return values). Machine learning models trained on labeled vulnerability

datasets predict defect density from these metrics. Semantic analysis using transformer-based code models (CodeBERT, GraphCodeBERT, or purpose-trained smart contract models) provides deeper understanding of code intent vs. behavior.

The security risk score combines defect density prediction with CVSS-adapted severity assessment. The financial impact estimate multiplies the probability of exploitation by the TVL at risk, adjusted for time exposure and detection probability.

## Registration and Operational Requirements

| Requirement | Minimum Threshold | Competitive Standard |
|---|---|---|
| **Registration Stake** | Minimum TAO set by subnet governance | Higher stake signals commitment; no direct emission advantage but affects validator trust |
| **Hardware — Track A** | 1x GPU (RTX 3090 class), 32GB RAM, SSD storage | Multi-GPU ensemble training server, high-speed NVMe storage, 64GB+ RAM |
| **Hardware — Track B** | 1x GPU (RTX 3090 class) for code model inference, 64GB RAM for large codebases | Dedicated code analysis GPU with 48GB+ VRAM for full transformer-based analysis |
| **Data Subscriptions** | Free on-chain sources only (viable but low accuracy ceiling) | Commercial oracle feeds + CVE database API + audit report corpus + alternative data |
| **Uptime** | 95% over rolling 7-day window | 99.5%+ with redundant infrastructure and automatic failover |
| **Response Latency** | Under 10 seconds for combined output | Under 3 seconds with pre-processing caches for known assets |
| **Chain Coverage** | Ethereum mainnet assets and contracts | Ethereum + Avalanche + Solana + Polygon + Arbitrum + BNB Chain |

# Validator Design — Verifying Two Ground Truths

Validators are the backbone of Nexara's integrity. Their role is more demanding than in most Bittensor subnets because they must maintain two completely separate verification infrastructure stacks and coordinate them into a single quality assessment. This complexity is both a barrier to entry and a source of validator competitive advantage — operators who build superior verification pipelines attract more delegation and earn more.

## The Three-Stage Evaluation Funnel

### Stage 1 — Quick Verification (New Miner Screening)

New miners entering the subnet are first evaluated on 5-10 asset/contract pairs where ground truth is quickly and unambiguously available. For Track A, this means highly liquid tokenized assets where price data is available within hours. For Track B, this means well-studied contracts with published audit reports where defect density ground truth is already established. Miners that cannot pass basic competence on either track are filtered out immediately, protecting the validator's evaluation resources.

### Stage 2 — Depth Evaluation (Breadth Testing)

Miners passing Stage 1 face expanded evaluation: 30+ asset/contract pairs spanning multiple chains, asset classes, and contract architectures. This tests genuine breadth of coverage. Evaluation includes newly deployed contracts (under 30 days old) where miners cannot have specifically prepared, ensuring that coverage claims are backed by genuine analytical capability.

### Stage 3 — Full Validation (Outcome Verification)

Full validation requires a minimum of three independent validators evaluating the same miner. Financial outcome verification waits for real market events. Code outcome verification uses a combination of audit report comparison, CVE matching, and exploit event monitoring. Only Stage 3 produces the consensus weights that determine TAO emission allocation.

## Financial Outcome Verification Infrastructure

The financial verification pipeline consists of: multi-source price oracle aggregation (minimum 3 independent oracle networks per asset), on-chain DEX trade data extraction for pricing ground truth, yield distribution monitoring from tokenized asset protocols, credit event monitoring from issuer announcements and on-chain governance records, and macro data feeds for contextual calibration.

Validators must implement cross-source consensus for all financial ground truth. Any oracle or data source whose value deviates more than two standard deviations from the multi-source median is flagged and excluded from that evaluation cycle. Validators whose verification pipelines rely on single-source data face competitive disadvantage in the delegation market.

## Code Outcome Verification Infrastructure

The code verification pipeline consists of: real-time CVE feed monitoring (NVD, MITRE, chain-specific security disclosures), exploit event detection from on-chain transaction monitoring (anomalous large withdrawals, flash loan patterns, multi-step attack sequences), audit report

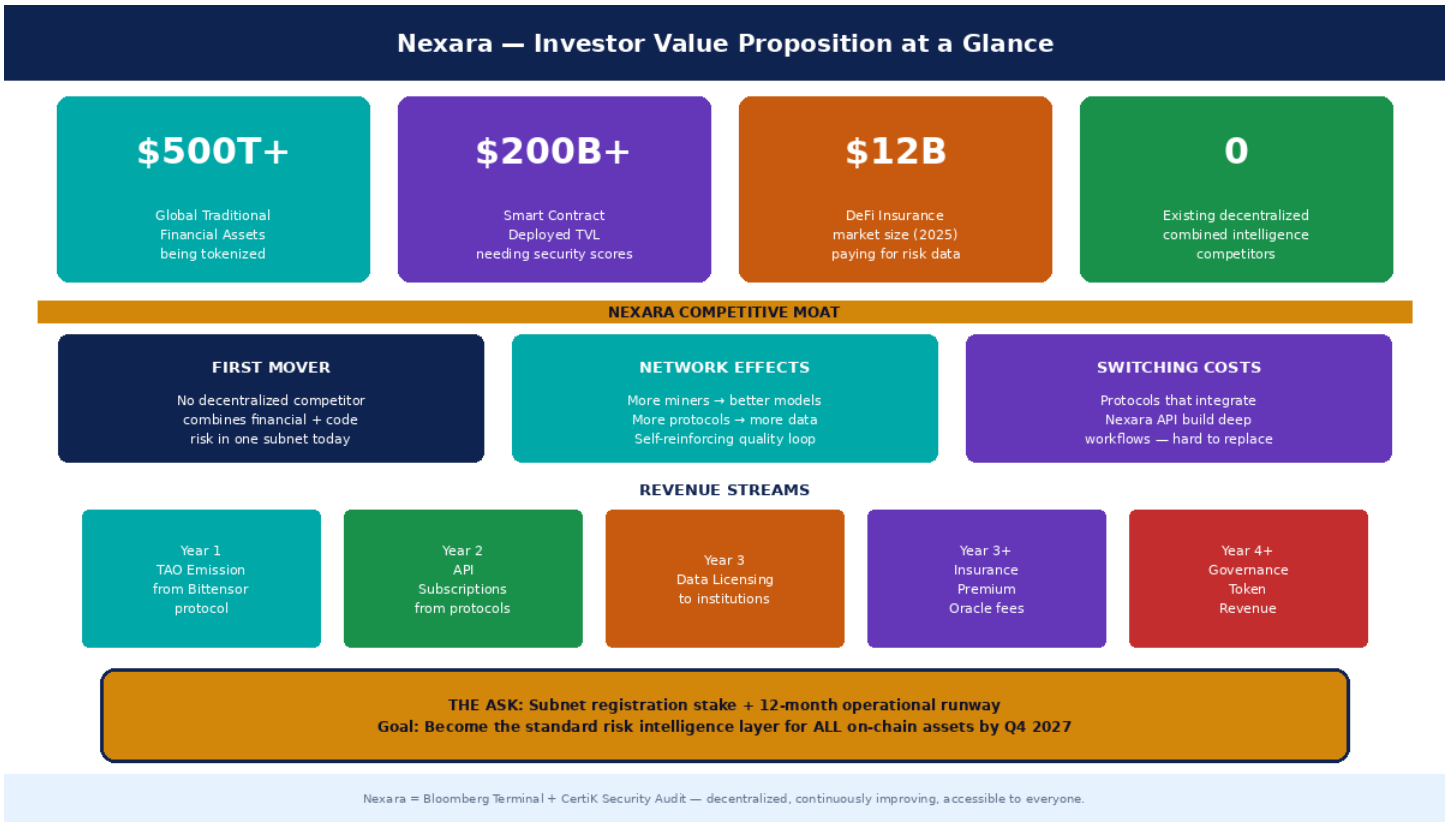
ingestion and parsing, bug bounty program disclosure tracking, and protocol upgrade monitoring to detect when code changes introduce new risk.

Code outcome verification has longer timelines than financial outcome verification. A smart contract may have high predicted defect density but not experience an exploit for months. Validators therefore maintain rolling evaluation windows: immediate verification on known vulnerability patterns; medium-term verification on newly deployed contracts monitored over 90 days; long-term verification on historical accuracy against the overall exploit event database.

## The Dual Verification Timing Challenge

> The most technically interesting design challenge in Nexara is managing the temporal mismatch between the two verification tracks.
>
> Track A (financial) can be partially verified in hours (pricing) to months (credit risk). Track B (code) can also be partially verified quickly (known vulnerabilities already in CVE databases) or may require months to years to verify (novel vulnerabilities that have not yet been publicly disclosed or exploited).
>
> Nexara handles this through tiered verification: miners earn partial weight credit as each verification tier completes, and full weight credit only when all applicable verification windows have closed. This prevents miners from gaming unverified dimensions while still providing timely feedback on verified dimensions.

# Business Logic and Market Rationale




## Why This Market, Why Now

Three macro trends are converging in 2026 to create the exact conditions that make Nexara viable and valuable: the RWA tokenization boom is bringing trillions in traditional assets on-chain; the DeFi smart contract exploit crisis is creating urgent demand for better security intelligence; and Bittensor's maturing subnet ecosystem provides proven infrastructure for competitive AI intelligence markets.

Each of these trends has been building for years, but they are reaching a critical inflection point simultaneously. The RWA market passed $10 billion in total tokenized value in 2024 and is projected to reach $100 billion by 2028. Smart contract exploit losses exceeded $2 billion in 2024. And Bittensor's subnet ecosystem now includes over 50 active subnets with proven product-market fit for competitive AI intelligence.

## Target Customer Segments and Willingness to Pay

| Customer Segment | What They Need From Nexara | Current Alternative | Willingness to Pay |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **RWA Lending Protocols** | Combined risk scores to set appropriate collateral ratios and interest rates | Manual due diligence, no continuous monitoring | High — directly affects protocol solvency |
| **DeFi Insurance Protocols** | Accurate premium pricing inputs for both asset default risk and smart contract exploit risk | Manual actuarial estimates, no code risk inputs | Very High — mispriced premiums are existential risk |
| **DAO Treasuries** | Portfolio monitoring, continuous risk alerts, yield optimization across RWA positions | Ad-hoc analysis, no systematic monitoring | Medium — governance-dependent, TAO-denominated fees align incentives |
| **Institutional Funds** | Auditable methodology for compliance, continuous monitoring for risk management, API integration with existing systems | Bloomberg + separate audits at $24K+/year + $50K+ per audit | High — institutional compliance requires comprehensive documented risk process |
| **Cross-Chain Bridges** | Smart contract security scoring for the contracts they are bridging assets through | One-time audits, no continuous monitoring | Medium-High — bridge exploits are catastrophic and frequent |

## Revenue Model — Three Phases

### Phase 1 (Year 1) — Emission-Funded Bootstrapping

Miners and validators sustain operations through TAO emission rewards from the Bittensor protocol. This model requires no external revenue and gives the ecosystem time to build quality and reputation before monetizing directly. Miners denominate operational costs in TAO where possible to reduce fiat exposure.

### Phase 2 (Year 2) — API Subscription Revenue

As Nexara establishes a track record of accurate intelligence, DeFi protocols begin paying TAO subscriptions for API access to Nexara scores. Pricing is determined by the market — protocols that rely heavily on Nexara intelligence pay more; protocols using it as a secondary signal pay less. This revenue supplements emission and reduces miner dependence on TAO price volatility.

### Phase 3 (Year 3+) — Institutional Data Licensing

Aggregated, anonymized Nexara intelligence — historical risk scores, prediction accuracy benchmarks, cross-chain security trend data — becomes a licensable data product for institutional research. This revenue stream scales independently of subnet participation levels and provides stable long-term income that can fund protocol development and security research initiatives.

# Competitive Landscape

An honest assessment of every alternative — centralized and decentralized — and exactly why Nexara occupies a position that none of them can easily replicate.

## Why No One Else Has Done This

The combination of financial intelligence and smart contract security intelligence sounds obvious in retrospect — of course a contract's security quality affects the financial risk of assets it holds. But building it requires crossing three separate expertise boundaries that rarely exist in the same team: deep financial modeling, smart contract security analysis, and decentralized protocol design. Nexara is explicitly designed to lower these barriers through open, competitive participation.

| Competitor | Their Strength | Their Gap | Nexara Advantage |
|---|---|---|---|
| **Bloomberg / Refinitiv** | Deep financial data breadth, trusted by institutions | No on-chain native support, no code analysis, $24K+/year minimum | Accessible, decentralized, combined score, on-chain native |
| **CertiK Skynet** | Continuous smart contract monitoring, real-time alerts | No financial risk integration, subscription model, centralized scoring | Financial + code combined, decentralized, outcome-verified accuracy |
| **Gauntlet Network** | Protocol risk modeling for DeFi governance parameters | Institutional-only pricing, no smart contract defect prediction, no RWA coverage | Open participation, both asset and contract coverage, permissionless |
| **DIA Protocol** | Decentralized price oracles for many assets | Price data only — no risk scoring, no code analysis, no yield prediction | Full intelligence stack across 6 dimensions, not just price |
| **OpenZeppelin Defender** | Smart contract monitoring and automation tools for developers | Developer tool only — no financial risk integration, no investor-facing scores | Investor-facing combined score, not just a developer tool |
| **Other Bittensor Subnets** | Proven Bittensor incentive architecture, established TAO ecosystem | None focus on financial + code intelligence combination for RWA assets | First mover in this specific combination within the Bittensor ecosystem |

# Go-To-Market Strategy

Nexara's go-to-market approach is designed around establishing credibility fast, integrating with high-visibility protocols, and creating switching costs through deep API integration before competitors can respond.

## Phase 1 — Prove the Intelligence (Months 1-4)

Before approaching any protocol for integration, Nexara needs to demonstrate that its intelligence is actually more accurate than what they currently use. The first four months focus entirely on building and publishing accuracy benchmarks: run the subnet in evaluation mode on historical data, publish accuracy metrics on past exploit events and credit events, and demonstrate that Nexara would have flagged the major DeFi hacks of 2023-2024 with statistically significant early warning signals.

This benchmark publication is the primary marketing asset. A well-documented, independently verifiable claim that Nexara predicted major exploit events with X% accuracy at Y days advance warning is more valuable than any sales pitch or white paper.

## Phase 2 — Land Anchor Integrations (Months 4-8)

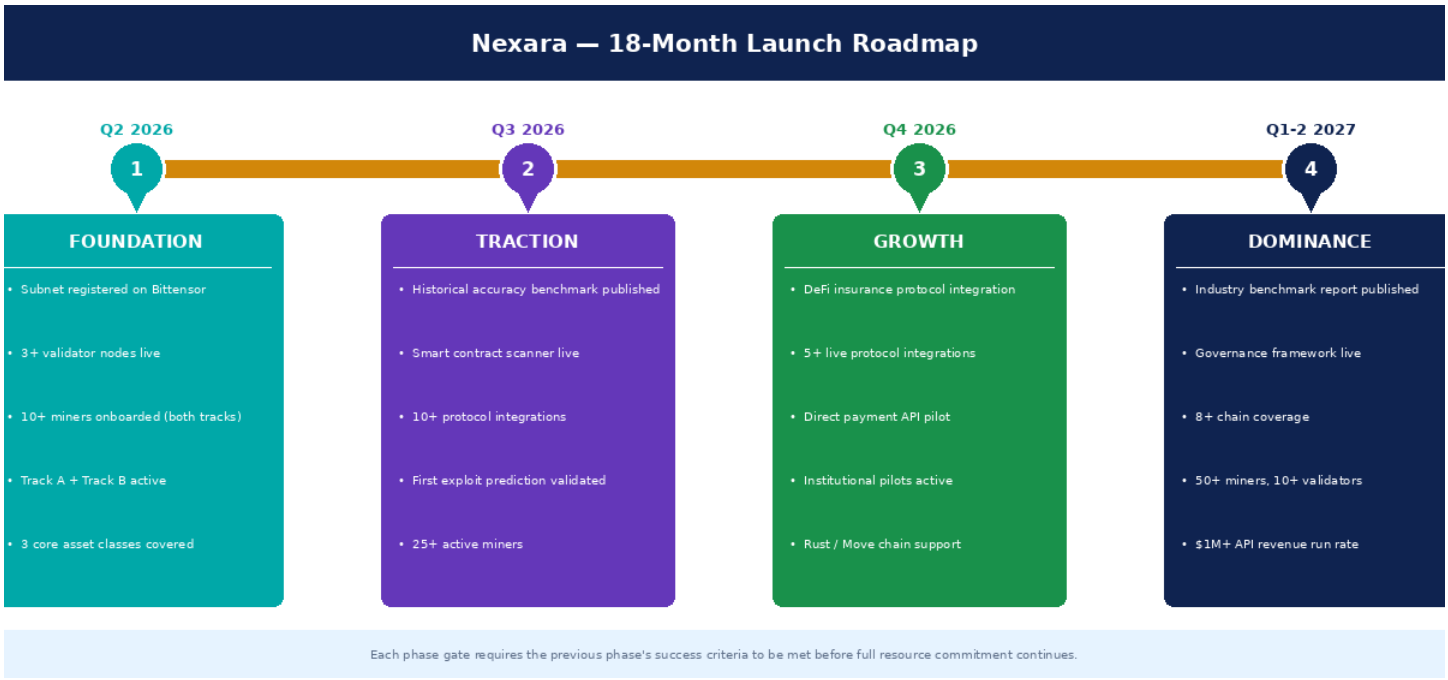
With accuracy benchmarks published, approach three target protocol categories for integration: one RWA lending platform (target: Maple Finance, Centrifuge, or Goldfinch), one DeFi insurance protocol (target: Nexus Mutual or InsurAce), and one DAO treasury management tool (target: Llama or Gnosis Safe). Offer free API access during integration in exchange for case study rights and public endorsement.

Anchor integrations create two critical assets: first-hand testimonials from credible DeFi protocol operators, and technical integration work (custom API endpoints, dashboard widgets, governance proposal templates) that creates real switching costs for those protocols.

## Phase 3 — Institutional Outreach (Months 8-18)

With live protocol integrations and published accuracy data, begin institutional outreach: family offices exploring DeFi yield, fund managers with RWA mandates, and corporate treasury teams allocated to digital assets. The pitch is simple: Nexara gives you Bloomberg-level financial intelligence plus CertiK-level security intelligence in one API call, at a fraction of the cost, with verifiable accuracy history.

# 18-Month Launch Roadmap




| Phase | Deliverables | Success Criteria |
|---|---|---|
| **Q2 2026 Foundation** | • Subnet registered on Bittensor mainnet<br>• 3+ validator infrastructure nodes live<br>• 10+ miners onboarded (both tracks)<br>• Track A: Ethereum RWA tokens covered<br>• Track B: Solidity contract scanner live | Stable evaluation cycles. Track A MAPE <3% on benchmark assets. Track B correctly flags 70%+ of contracts with known CVEs in holdout test set. |
| **Q3 2026 Traction** | • Historical accuracy benchmark report published<br>• Rust/Move contract analysis added (Solana/Sui)<br>• First anchor protocol integration live<br>• 25+ miners competing on subnet | Benchmark report downloaded by 500+ DeFi operators. At least one protocol publicly using Nexara for risk management decisions. |
| **Q4 2026 Growth** | • DeFi insurance protocol integration live<br>• 5+ protocol integrations total<br>• Direct payment API pilot launched<br>• Institutional outreach programme active | 5+ live integrations. Direct API revenue covering 20%+ of miner operational costs. First institutional client onboarded. |
| **Q1-2 2027 Dominance** | • Industry benchmark report: Nexara vs CertiK vs Moody's<br>• Governance token and subnet governance live | Recognised as the standard combined risk intelligence layer for at least 3 major RWA protocols. $1M+ annualised API subscription revenue. |

| | | |
|---|---|---|
| | • Cross-chain coverage: 8+ EVM and non-EVM chains<br>• 50+ miners, 10+ validators on subnet | |

# Risk Analysis and Mitigation

## Technical Risks

### Risk: Track B Verification Lag

Smart contract vulnerabilities may not be publicly disclosed for months or years after they exist in code. This means Track B verification windows are long and uncertain, creating slow feedback loops for miners trying to improve their code intelligence models.

Mitigation: Tiered verification system — miners earn partial weight credit from known CVE matching immediately, and longer-term credit as novel exploits confirm or deny predictions. Community-developed datasets from audit reports and bug bounty disclosures supplement CVE data for shorter verification cycles.

### Risk: Code Language Diversity

Smart contracts are written in Solidity (Ethereum), Rust (Solana, Near), Move (Aptos, Sui), and Vyper (Ethereum). Miners need separate analysis models for each language, creating significant development overhead.

Mitigation: Launch with Solidity coverage only (covering 80%+ of TVL). Add Rust and Move in subsequent quarters. Miners that support only Solidity still earn competitive emission on Ethereum assets — full cross-chain coverage is a premium capability.

## Market Risks

### Risk: Exploit Events Damaging Reputation

If a major smart contract exploit occurs for a contract that Nexara miners had scored as low-risk, it could damage the subnet's credibility, even if the exploit used a novel attack vector that no existing analysis could have detected.

Mitigation: Publish clear methodology documentation explaining the scope and limitations of Track B analysis. Distinguish between known vulnerability patterns (where high accuracy is achievable) and novel zero-day attacks (where statistical impossibility of prediction should be honestly communicated). Frame Nexara as risk-reduction intelligence, not security guarantee.

### Risk: Centralized Competitors Respond

If Nexara demonstrates strong product-market fit, CertiK, Gauntlet, or a new entrant could develop a competing combined intelligence product.

Mitigation: First-mover advantage in protocol integrations creates switching costs. Network effects — more miners producing better models — create accuracy advantages that are difficult to replicate quickly. The decentralized, open participation model provides a different value proposition than centralized competitors regardless of feature parity.

## Ecosystem Risks

### Risk: TAO Token Price Volatility

Severe TAO price decline could make miner economics unsustainable, causing talent and infrastructure exodus from the subnet.

Mitigation: Accelerate transition to direct TAO payment model in Year 2 to create utility-based demand for TAO independent of speculative price. Structure miner costs in TAO where possible. The dual-track value proposition — serving both security and financial intelligence markets — diversifies demand for the subnet's outputs.

# Team and Expertise Requirements

Successfully launching and operating Nexara requires a team that spans three distinct expertise domains. This section describes the ideal team composition for both the founding launch team and the broader community of miners and validators.

## Core Founding Team Requirements

| Role | Required Skills | Responsibilities |
|---|---|---|
| **Bittensor Protocol Engineer** | Deep Bittensor/Subtensor knowledge, Python, Yuma Consensus implementation, subnet deployment experience | Subnet registration, validator/miner API design, Yuma weight pipeline, emission mechanics implementation |
| **Smart Contract Security Researcher** | Solidity/Rust security, CVE analysis, static analysis tools (Slither, Mythril), CVSS scoring methodology | Track B model architecture, ground truth dataset curation, verification pipeline for code outcomes |
| **Financial AI Engineer** | Quantitative finance, time series modeling, credit risk models, DeFi protocol mechanics, oracle integration | Track A model architecture, financial data pipeline, yield and pricing model development, calibration methodology |
| **DeFi Protocol Integrations Lead** | Solidity development, API design, DeFi ecosystem relationships, smart contract integration patterns | Protocol partnership development, API specification, integration documentation, pilot programme management |
| **Data Infrastructure Engineer** | Data pipeline engineering, oracle network integration, database architecture, multi-chain data extraction | Unified data infrastructure serving both tracks, oracle integration, real-time monitoring systems |

## Miner Community Requirements

Nexara will attract the strongest miners from three communities: quantitative finance professionals who understand financial risk modeling, smart contract security researchers who have experience with vulnerability analysis, and AI/ML engineers who can train large-scale prediction models. Miners who bridge two or more of these communities will have the strongest competitive positions. Actively recruiting across all three communities — through hackathons, academic partnerships, and the DeFi security research community — is a key go-to-market activity.

# Tokenomics and Funding Ask

## How TAO Flows Through Nexara

Nexara uses Bittensor's native TAO token for all economic activity. There is no additional token. This is an intentional design choice: introducing a new token would create regulatory risk, liquidity fragmentation, and governance complexity that is unnecessary when Bittensor's existing economic infrastructure is well-suited to the subnet's needs.

| Economic Activity | How TAO Is Used | Who Benefits |
|---|---|---|
| **Miner Registration** | Minimum stake deposited as security commitment. Slashed for severe violations. | Protocol — stake creates skin-in-the-game for miner quality |
| **Validator Registration** | Stake deposited and locked. Higher stake = more influence within clipping bounds. | Protocol and delegators — stake aligns validator incentives with honest evaluation |
| **Emission Rewards** | TAO released each block, distributed proportionally to miner consensus weights | Miners (majority) and validators (base reward + delegation share) |
| **Delegation** | TAO holders stake with validators to earn a share of validator rewards | Delegators and validators — creates validator quality competition |
| **API Subscriptions (Phase 2)** | DeFi protocols pay TAO for access to Nexara intelligence via API | Miners and validators through additional reward distribution |

## The Funding Ask

Nexara is seeking seed investment to cover the following launch costs:

- Subnet Registration: The Bittensor protocol requires a TAO stake to register a new subnet. This is the primary blockchain-level cost.
- Validator Infrastructure (3 nodes, 12 months): Professional-grade servers with redundant connectivity for the initial validator set. Estimated $8,000-$15,000 per month per validator node.
- Core Team Salaries (12 months): 5 full-time roles as described in the Team section above, plus advisors.
- Miner Recruitment Incentives: Grants and hackathon prizes to attract the first 20+ high-quality miners across both tracks. Estimated $200,000 in TAO-denominated grants.
- Data Infrastructure: Premium financial data subscriptions, CVE database access, and audit report corpus licensing for the founding validator and miner team.
- Marketing and Protocol Partnerships: Conference presence, DeFi ecosystem outreach, and anchor integration support.

In exchange, investors receive equity in the operating entity (or SAFE for early-stage), plus strategic advisory rights that include governance input on initial subnet parameters. No proprietary token is issued.

# Frequently Asked Questions

These are the questions investors, potential miners, and DeFi protocol operators ask most often.

## For Investors

### Q What is the exit strategy for investors?

Three potential paths: (1) Protocol acquisition — established financial data providers (Bloomberg, Refinitiv, Moody's) or blockchain security firms may acquire Nexara as their decentralized intelligence arm. (2) Token launch — if Nexara demonstrates strong product-market fit, a governance token launch becomes viable, providing liquidity for early equity holders. (3) Revenue-generating business — the API subscription and data licensing model can produce cash flows that support traditional buyback or dividend structures within the operating entity.

### Q Why is Bittensor the right infrastructure rather than building a standalone protocol?

Bittensor provides three things that would take years to build independently: proven Yuma Consensus for fair AI evaluation without central arbitration, an existing community of miners and validators with the hardware and expertise to join immediately, and established TAO token liquidity for rewarding participants. Building a new incentive protocol from scratch would cost millions and take 2-3 years. Bittensor lets us focus on the intelligence problem, not the infrastructure problem.

### Q How do you prevent miners from colluding with the protocols they are scoring?

The evaluation architecture creates structural separation. Miners do not choose which assets to evaluate — validators select them randomly from a rotating pool. Miners do not know in advance which specific contracts will be queried. Most importantly, outcomes are verified against real-world events (actual exploits, actual defaults) that are outside any miner's ability to manipulate. A miner could bribe a small protocol to not report a bug — but they cannot prevent a CVE from being published or a major exploit from appearing on-chain.

## For Potential Miners

### Q I am a smart contract security researcher with no finance background. Can I still mine profitably?

Yes — Track B is your competitive advantage. The composite scoring system requires competence in both tracks, but a miner who excels on Track B while maintaining baseline competence on Track A will outperform miners who are strong on Track A but weak on Track B. The security research community is currently underrepresented in Bittensor subnets, which means Track B specialists will face less competition initially. Consider partnering with a quant finance expert to cover Track A while you focus on Track B.

### Q How long does it take to build a competitive miner for both tracks?

Track A: 4-8 weeks to build a baseline model using open-source financial data. 3-6 months to develop a genuinely competitive model with premium data sources and ensemble methods. Track B: 6-12 weeks to build a functional Solidity static analysis pipeline. 4-6 months to

develop competitive defect density prediction with a well-curated training dataset. Plan for 4-6 months from starting development to being competitive on both tracks simultaneously.

### Q What happens to my staked TAO if my model performs poorly?

Poor model performance reduces your emission share — you earn less TAO. Your staked TAO is NOT slashed for poor predictions. Slashing only occurs for severe violations: refusing to respond to evaluation queries, submitting malformed outputs designed to break validators, or demonstrable manipulation attempts. Honest but inaccurate predictions are penalized economically through reduced emission, not through loss of staked capital.

## For DeFi Protocol Operators

### Q How accurate is Nexara's smart contract security scoring compared to professional audits?

An honest comparison: professional audits by top firms find more novel vulnerabilities, especially in new protocol designs that have no historical precedent. Nexara is better at continuous monitoring, known vulnerability pattern detection, and rapid assessment of newly deployed contracts. The ideal use case combines both: get a professional audit for launch, and use Nexara for continuous monitoring and rapid assessment of contract upgrades. Nexara is not an audit replacement — it is continuous intelligence between audits.

### Q How do we integrate Nexara intelligence into our protocol's risk parameters?

Nexara outputs a structured API response with six fields: price, yield, credit risk score, defect density, security risk score, and financial impact estimate — plus confidence intervals for each. Your protocol can use these directly as inputs to governance parameters (collateral ratios, interest rates, coverage limits) or as dashboard data for human decision-makers. Integration documentation, sample code for major smart contract platforms, and integration engineering support will be available from the Nexara team during the launch phase.

# Nexara

*Decentralized Dual-Intelligence Subnet for Bittensor*

Combining Real-World Asset Intelligence with Smart Contract Defect Prediction

February 2026 | CONFIDENTIAL