Tokenomics research and Nightshade design options

Date: 2026-05-25 **Status:** Research synthesis + first-pass design options. NOT a binding decision; informs an eventual D-013-style entry in `DECISIONS.md` once the strategic opportunity that motivated this research is concrete and counsel-reviewed. **Scope:** Hyperliquid HYPE deep dive + comparative scan of 12 protocols + tokenomics-primitives pattern extraction + 5 Nightshade-specific design options + legal framing under the March 2026 SEC interpretation. **Authority:** Claude research + synthesis under James's direction 2026-05-25; primary-source verification by 5 parallel research sub-agents. Sources cited inline; unverified claims explicitly flagged.

> ■■ ***Alignment note (2026-06-28) — read first.*** *This is a dated research/design record. A later decision changes part of it; the canonical current source is `DECISIONS.md` (D-013). -* ***The 5,000 XMR mint-fee cap was removed entirely (D-013, 2026-06-28).*** *The mint fee is uncapped, so any cap-dependent analysis below is moot — in particular* ***§5.3 "Option C — Endowment for Post-Cap Registration"*** *(there is no post-cap phase), the "0.027182 XMR mint fee with 5000 XMR cap" framing in §5, and the §17.10 post-cap admission question. The buyback analysis (rejecting fee-funded buyback on securities grounds) still stands and is reflected in the live design.*

---

0. Why this document exists

James surfaced 2026-05-25 that an opportunity has come up that would require some form of native token integration with Nightshade. Rather than designing reactively, we did a wide survey of how production token economies actually work — Hyperliquid (the primary research target), plus burn-and-mint protocols (Helium / Filecoin / Render / Akash / Arweave), plus vote-escrow and fee-distribution protocols (GMX / Curve / Lido / Frax / Pendle / dYdX v4 / Ondo) — and extracted the recurring primitives so the eventual Nightshade design is informed by what's worked, what's failed, and what's drawn regulatory attention.

This document captures both the research findings and a first-pass set of Nightshade-specific design options. It does NOT recommend a single approach — that depends on the specific opportunity, which is unresolved at the time of writing (see §6).

The earlier legal-surface conversation (memory + `docs/session-2026-05-25-summary.md` Cycle 7) applies as background to this entire document. A token formalizes parts of that legal surface; counsel engagement before any public token launch is binding per the dev plan §15 communication discipline.

---

1. Hyperliquid (HYPE) — verified deep dive

1.1 Supply (caveat: 1B figure is community-reported, not docs-verified)

- **Max supply: 1,000,000,000 HYPE** — reported by multiple primary-adjacent channels citing the Hyper Foundation's genesis blog post and X posts; **could NOT be retrieved from the official gitbook**. The gitbook has no dedicated tokenomics page (confirmed via llms.txt index).
- **Initial circulating at TGE Nov 29, 2024: 310M HYPE** (the genesis airdrop, fully unlocked at TGE). Same caveat — sourced from Hyper Foundation channels.

1.2 Allocation (per Hyper Foundation blog as reported by secondary outlets)

Bucket	%	Tokens
Future Emissions & Community Rewards	38.888%	~388.88M
Genesis Distribution (airdrop)	31.0%	310M
Core Contributors	23.8%	238M
Hyper Foundation Budget	6.0%	60M
Community Grants	0.3%	3M
HIP-2 Hyperliquidity	0.012%	~120k

Verified directly: staking rewards come "from the future emissions reserve" (staking docs). The allocation table itself is NOT on the gitbook — treat as widely-reported but not docs-verified.

Core contributor vesting: widely reported as 1-year cliff (through Nov 29, 2025), then linear unlock to 2027–2028. NOT verified on primary docs.

No VC / no presale: verified — core-contributors doc states "Hyperliquid Labs is self-funded and has not taken any external capital."

1.3 The Assistance Fund (the load-bearing mechanism)

- **Address:** `0xfefefefefefefefefefefefefefefefefefefefe` (verified in primary docs).
- **Mechanism (verified):** trading fees auto-convert to HYPE as part of L1 execution; HYPE in the AF is burned; tokens permanently removed from circulating + total supply.
- **Fee percentage to AF:** the official fees page states only that "fees are entirely directed to the community (HLP, the assistance fund, and deployers)." The widely-cited **~97% figure is NOT on the gitbook** — flag as unverified.

- **Formal burn governance vote:** verified via Hyper Foundation X post — 85% for, 7% against, 8% abstaining on stake-weighted vote.

The AF is HYPE's signature mechanism: protocol fees → HYPE buy → burn. Cleanly automated. Demonstrably destructive of supply. Also the single highest-risk feature under the March 2026 SEC framework (§4 below).

1.4 HyperCore vs HyperEVM

- **HyperCore:** fully on-chain perp DEX + spot DEX + CLOB under HyperBFT consensus (a HotStuff variant). Published performance: 0.2s median end-to-end latency, 0.9s p99, ~200k orders/sec throughput. Perp/spot quote asset is USDC.
- **HyperEVM:** EVM L1, chain ID 999 mainnet / 998 testnet. Cancun without blobs. EIP-1559 enabled; **both base and priority fees burn** (priority fees sent to zero address). HYPE is the native gas token.
- **Bridging:** HYPE Core → EVM via sending HYPE to system address `0x2222222222222222222222222222222222222222`.
- **Mainnet launch (HyperEVM):** Feb 18, 2025 per secondary reporting (The Block, BanklessTimes); inherits HyperBFT security.

1.5 HIP-1 (spot deployment) — verified

- **Dutch auction:** 31 hours duration; linear decay from `initial_price` → 500 HYPE floor.
- `initial_price` = 500 HYPE if last auction failed; otherwise 2× last clearing price.
- **Denominated in HYPE since May 22, 2025** (previously USDC).
- Six parameters per token: `name` (≤6 chars, no uniqueness constraint), `weiDecimals`, `szDecimals` (constraint `szDecimals + 5 ≤ weiDecimals`), `maxSupply`, `initialWei`, `anchorTokenWei`.
- Each HIP-1 token auto-spins up a native USDC-quoted order book on HyperCore.

1.6 HIP-2 (Hyperliquidity) — verified

- Fully on-chain auto-market-making strategy executed in block-transition logic ("no operators").
- 0.3% spread guaranteed; updates every ≥3 seconds.
- Price ladder: `px_i = round(px_{i-1} * 1.003)`.
- Deployers fund with USDC (not HYPE); HIP-2 is configured at HIP-1 deploy time.
- Coexists with the same native CLOB used by HIP-1 — external MMs can post tighter inside quotes.

1.7 HIP-3 (builder-deployed perpetuals) — verified

- Permissionless deployment of perp DEXes; inherits HyperCore matching/margining.

- **Stake requirement:** 500,000 HYPE locked ≥183 days post-deployment. Slashable.
- First 3 assets per DEX free; additional assets via Dutch auction.
- Deployer configures fee share 0–300% (0–100% in "growth mode"); above 100%, protocol fee scales up.
- Slashing via stake-weighted validator vote: up to 100% for invalid state transitions; up to 50% for prolonged downtime; up to 20% for performance degradation.

1.8 Validator economics — verified

- **Active set:** top 24 validators by stake.
- **Min self-bond:** 10,000 HYPE, locked 1 year.
- **Delegation lockup:** 1 day per validator.
- **Unstaking queue:** 7 days, max 5 pending per address.
- **Commission:** validators charge commission; increases capped at ≤1% delta.
- **Slashing:** "reserved for provably malicious behavior such as double-signing"; currently NO automatic slashing implemented.
- **Reward formula:** inverse-sqrt of total staked, Ethereum-inspired. At 400M HYPE staked, ~2.37%/yr from the future emissions reserve. Accrued every minute; distributed daily; auto-compounded.
- **Foundation Delegation Program:** requires KYC/KYB; restricted jurisdictions explicitly listed (US, Ontario, Cuba, Iran, Myanmar, NK, Syria, Russian-occupied Ukrainian regions). Operators must run ≥2 non-validator nodes at 95% uptime. **This is a deliberate jurisdictional firewall.**

1.9 Launch design (Nov 29, 2024, 07:30 UTC)

- 31% of 1B supply pushed to ~94,000 wallets in genesis airdrop (recipient count is secondary-reported, not docs-verified).
- Eligibility: points-based from testnet trading, mainnet activity, and referrals across 2023–2024. Anti-sybil via trading-volume weighting + team-curated point reductions.
- All genesis tokens fully unlocked at TGE — eliminates the unclaimed-supply leakage common to vested airdrops.
- The "no-VC, fair-launch" narrative rests on: zero private sale, no allocation to outside investors, push-distribution to actual traders.

1.10 What makes HYPE work — analytical distillation

Five primary mechanisms drive HYPE's value capture:

1. **No-presale genesis** eliminates the Telegram/Kik enforcement pattern (pre-sale → securities offering).
2. **Gas burn on HyperEVM** ties chain activity to passive supply contraction.

3. **Assistance Fund** automates fee-funded buyback + burn at L1 execution level.
4. **HIP-1 auction** consumes HYPE every time a new spot listing deploys.
5. **Validator/HIP-3 lockups** structurally remove HYPE from circulation.

The genuinely-novel mechanism is the AF — it's the cleanest implementation of "protocol fees fund native-token destruction" that's automated, on-chain, and demonstrably destructive of supply. Also the single most legally exposed feature under the new SEC framework (§4).

1.11 Unverified items flagged

1. The 1B max supply figure has no dedicated gitbook page.
2. The full allocation % table (38.888 / 31 / 23.8 / 6 / 0.3 / 0.012).
3. The "~97% of fees to AF" claim — docs say only "entirely directed to the community."
4. Core contributor cliff/vesting end dates.
5. Number of airdrop recipients (~94k) and median grant size.
6. Cumulative AF HYPE bought + burned to date.
7. Auction clearing prices in HYPE for recent HIP-1 deployments.

Primary sources lean toward a "trust the X account + community wiki for tokenomics specifics" pattern — the official gitbook is heavy on technical mechanics and light on distribution accounting.

---

2. Comparative scan — 11 protocols, one paragraph each

2.1 Helium (HNT)

Burn-and-mint equilibrium. HNT is burned to mint non-transferable **Data Credits** pegged at $0.00001 USD each; HNT/DC conversion rate floats with HNT's oracle price. Following HIP-70 (Aug 2022), migrated to Solana on April 18, 2023. **HIP-138** (approved Nov 22, 2024) ended IOT/MOBILE emissions; since January 2025 all hotspot rewards are paid in HNT. **Demand:** DC burn for IoT/5G data and onboarding fees. **Supply pressure:** scheduled HNT emissions to hotspots (third halving August 2025). **Failure mode:** the original subDAO design (HIP-51) was abandoned because DC burn was tiny relative to IOT/MOBILE emissions, leaving subDAO tokens structurally inflationary — exactly the gap HIP-138 was designed to fix. **The central lesson for any BME design: emissions to suppliers must not outpace consumer burn or the whole structure collapses.**

2.2 Filecoin (FIL)

Storage Provider **Initial Pledge** = Storage Pledge (~20 days of expected sector block reward) + Consensus Pledge (30% of circulating supply × sector share of QAP / max(baseline, total QAP)). Verified deals (FIL+) grant a **10× QAP multiplier** — 100 TiB of verified data counts as 1 PiB of power, earning 10× block rewards but requiring 10× collateral and exposing 10× slashing. Block rewards: 25% liquid immediately, 75% vested linearly over 180 days. **Demand:** FIL locked as collateral, deal fees, gas. **Supply pressure:** block rewards. **Failure mode:** the 10× multiplier financialized FIL+ DataCap into a quasi-yield product; FIP-0080 explicitly proposes scheduled reductions to the FIL+ quality multiplier because the subsidy was not producing proportional real-storage utility. **Lesson: subsidies designed to align utility can become detached financial instruments.**

2.3 Render (RNDR/RENDER)

RNP-001 introduced the Burn-and-Mint Equilibrium model (jobs paid in fiat-priced tiered "Render Credits" burn RENDER on the artist side; new RENDER minted to node operators). RNP-002 (March 2023) authorized migration from Ethereum ERC-20 RNDR to Solana SPL RENDER; executed November 2, 2023. **Demand:** USD-priced render-job burns. **Supply pressure:** emissions to node operators + treasury unlocks. **Failure mode:** real on-chain burn volume has been small relative to market cap, and OTOY (the founding company) still effectively controls the rendering software and credit pricing, making the BME flow dependent on a single off-chain operator. **Lesson: BME requires both (a) demonstrable consumption pressure and (b) decentralized supply of the underlying service.**

2.4 Akash (AKT)

Reverse-auction compute leases settled via on-chain escrow. AKT 2.0 introduced a **take rate**: 4% on AKT-denominated leases, 20% on USDC-denominated leases — the rate gap was designed to push settlement to AKT but instead pushed it to USDC. **Demand:** AKT as preferred lease currency (heavily subsidized); staking for validator security. **Supply pressure:** validator inflation rewards + provider sell-through. **Failure mode:** real daily compute spend is reportedly only ~$8K–$12K/day, a small fraction of AKT's mcap; the 20% USDC tax pushed most settlement off the native token, weakening the demand link the 4% AKT rate was meant to create. **Lesson: discount-based demand tools rarely beat denominator inertia.**

2.5 Arweave (AR)

One-time upload fee priced for **200 years of replicated storage at today's costs**; spillover deposited into the **Storage Endowment** that pays miners over time. Consensus is SPoRA (Succinct Proofs of Random Access) — miners must prove access to a randomly selected historical chunk. **Demand:** AR burned/locked at upload to fund endowment. **Supply pressure:** miner payouts from endowment + inflation. **Failure mode:** endowment is solvent only if storage costs continue declining ≥0.5%/yr (vs Kryder's historical ~30–38%/yr). If real-cost decline stalls — NAND price floors, energy cost increases, replication-factor pressure — the endowment underfunds long-tail data. **Lesson: endowment models can offer the cleanest "consumptive" legal framing but are highly sensitive to a single macroeconomic assumption.**

2.6 GMX (GMX) + esGMX

Triple-reward staking: staked GMX accrues (1) ETH/AVAX fees, (2) esGMX (escrowed, non-transferable), and (3) Multiplier Points at fixed 100% APR. esGMX vests linearly over 365 days back to GMX; vest requires the average GMX/GLP used to earn the esGMX to be reserved (capital-locked vest). **GMX v2:** 27% of platform fees buy back GMX from open market and distribute to stakers (replacing pre-v2 direct ETH fee share). **Demand:** triple-reward staking. **Supply pressure:** esGMX vesting unlocks. **Failure mode:** Multiplier Points are burned proportionally on unstake — a loyalty trap. Active governance proposal (Oct 2025) would redirect the 27% buyback toward GM pools, which would gut the staker demand sink. **Lesson: fee-buyback-distribute creates the strongest staker demand AND the strongest securities profile.**

2.7 Curve (CRV) + veCRV

Lock CRV up to 4 years → veCRV (linearly decaying), granting governance + gauge weight votes. Locks are non-transferable and irrevocable. **Demand:** veCRV captures 50% of pool admin fees (now converted to crvUSD weekly) and 80% of crvUSD market interest. LPs additionally get up to 2.5× boost on CRV emissions based on their veCRV share. **Supply pressure:** weekly CRV emissions to gauges. **Failure mode:** Convex (cvxCRV) controls roughly ~53% of locked veCRV — governance capture risk. Bribes via Votium effectively financialized governance. **Lesson: vote-escrow concentrates governance into the hands of whoever solves the lock-illiquidity problem first.**

2.8 Lido (LDO)

LDO is **pure governance** — controls node operator set, the 10% protocol fee on staking rewards, and parameters. As of 2025, **Dual Governance** is live: stETH holders can submit "exit signals" that dynamically extend the LDO timelock; at >1% TVL signaled, timelock grows; at >10%, "rage-quit" blocks execution until exit completes. **Demand:** weak — LDO has no fee accrual; demand is solely governance utility + speculation. **Supply pressure:** treasury distributions, vested team/investor unlocks. **Failure mode:** LDO market cap is structurally divorced from $38B+ stETH TVL because no value accrues to the token. Compounding: a **late-2024 SDNY ruling (Samuels v. Lido DAO) classified the DAO as a general partnership**, exposing LDO holders to potential securities liability. **Lesson: pure governance is NOT a legal safe harbor — the Samuels ruling is the cautionary precedent that broke this assumption.**

2.9 Frax (FXS → FRAX rebrand)

veFXS modeled on veCRV — variable lock for voting power + farming boost. FXS emissions halve annually. **Frax v3 has deprecated the fractional-algorithmic design**; FRAX targets 100% collateralization via AMOs + RWAs. **Demand:** sFRAX (ERC-4626 vault) distributes protocol yield weekly, anchored to Fed IORB rate (initially 10%, designed to converge to ~5.4% IORB). veFXS receives surplus protocol revenue from frxETH staking, Fraxlend, and FRAX operations. **Supply pressure:** FXS emissions (halving). **Failure mode:** FRAX briefly de-pegged during March 2023 USDC crisis. The 2025 "Fraxtal North Star" rebrand (FXS → FRAX, veFXS → veFRAX) introduces ticker-confusion risk. **Lesson: algorithmic backing failed publicly; the model converged to RWA-collateralized + IORB-anchored which is closer to a wrapped TradFi money market than DeFi.**

2.10 Pendle (PENDLE) + vePENDLE

Yield tokenization splits a yield-bearing asset (stETH, sUSDe, LRTs) into **PT (principal, redeemable 1:1 at maturity)** and **YT (rights to all yield until maturity)** — enabling fixed-yield and leveraged-yield trades on the same underlying. **Demand:** vePENDLE (max lock 2 years, linear decay to zero) captures 80% of swap fees of pools they vote on, plus ~3pp of YT yield (Pendle takes a 5% cut, of which 3pp goes to vePENDLE). **Supply pressure:** PENDLE weekly emissions to gauges. **Failure mode:** revenue structurally tethered to the yield-bearing-asset narrative — Pendle TVL ballooned on Ethena sUSDe / LRT points farming; revenue concentration risk if those narratives unwind. **Lesson: yield-tokenization protocols are levered bets on whatever yield-bearing trend dominates that quarter.**

2.11 dYdX v4 (DYDX, Cosmos appchain)

Sovereign Cosmos appchain with **off-chain orderbook, on-chain settlement**. Trading fees paid in **USDC** flow through the Cosmos staking-distribution module to validators + DYDX stakers. **Demand:** all trading fees + gas fees, minus validator commission and community tax (0%), distribute as `(staked / total_staked) × (1 − validator_commission)`. **Supply pressure:** ethDYDX → native DYDX migration was one-way, no new emissions to stakers (rewards are USDC). Pre-existing investor/team unlocks remain a supply overhang. **Failure mode:** USDC-denominated rewards directly to DYDX stakers create the **strongest "security-like" profile of any token in this sample** — fees flow from third-party traders to passive token holders, classic Howey-test pattern. **Lesson: routing fees-in-foreign-currency to passive stakers is the single most legally exposed model in this sample.**

2.12 Ondo (ONDO)

ONDO is **purely a governance token** for the Ondo DAO. **Deliberate two-entity split:** Ondo Foundation (governance/DAO) is distinct from Ondo Finance, Inc. (corporate entity operating OUSG, USDY). Per Ondo Foundation docs: ONDO "does not convey ownership or revenue rights in Ondo Finance, Inc. or in any tokenized asset products." OUSG (BlackRock BUIDL-backed) and USDY (T-bill backed, ~5.2% APY) deliver yield to **product holders**, not to ONDO holders. 10B total supply, no inflation, ~52.1% ecosystem / 33% protocol development / 12.9% private sale / 1.99% community. **Demand:** governance only. **Supply pressure:** vesting unlocks through 2029. **Failure mode:** governance shell sits atop a profitable RWA business with no contractual cash-flow claim — value extraction depends entirely on a future "fee switch" DAO vote the corporate entity could resist. **Lesson: the Foundation/Operations split is the explicit defensive STRUCTURE Lido lacked — Ondo is the model for legally-conservative protocol token design despite the weak demand profile.**

---

3. Six recurring tokenomics primitives

Extracted across the 12 projects. Each primitive: definition, pioneer/refiner, demand driver, supply sink, failure mode, legal exposure.

3.1 Burn-and-mint equilibrium (BME)

- **Definition:** consumers burn the native token to obtain a fiat-pegged unit of account that pays for service consumption; new tokens minted as emissions to suppliers.
- **Pioneer:** Helium HNT/DC. Refined by Render.
- **Demand:** service consumption.
- **Supply sink:** token burn per unit.
- **Failure mode:** supplier emissions outpace consumer burn → structurally inflationary (HIP-138 lesson).
- **Legal exposure:** Moderate. Utility usage is clear; if emissions look like "investment returns" → exposure. Helium has not drawn enforcement; Render has not either.

3.2 Collateralized service provision

- **Definition:** service providers post collateral in the native token; slashable for misbehavior or service failure.
- **Pioneer:** Filecoin.
- **Demand:** to earn the service-provision revenue, providers must acquire and lock token.
- **Supply sink:** locked collateral; not destroyed but unavailable to sell-side.
- **Failure mode:** subsidies designed to encourage quality (FIL+ 10× multiplier) get financialized into yield products (FIP-0080 walk-back).
- **Legal exposure:** Low if collateral is genuinely at risk; high if it's effectively a yield product.

3.3 Vote-escrow (ve-tokens)

- **Definition:** lock token for time → governance + boost + (often) fee share.
- **Pioneer:** Curve. Refined by Frax, Pendle, Balancer.
- **Demand:** governance + boost + fee accrual.
- **Supply sink:** time-locked (4-year max typically).
- **Failure mode:** aggregator capture (Convex pattern) — a layer-2 protocol solves the lock-illiquidity problem and accumulates governance share.
- **Legal exposure:** Variable. Pure governance with no fee accrual = lower exposure; fee accrual to lockers = closer to security.

3.4 Buyback-and-burn from fees

- **Definition:** protocol fees automatically buy the native token on open market and burn the bought tokens.

- **Pioneer:** Binance BNB (quarterly buyback), refined by Hyperliquid AF (continuous, on-chain at L1 execution).
- **Demand:** holders benefit from fee-driven price support + supply destruction.
- **Supply sink:** bought tokens burned.
- **Failure mode:** none mechanical — failure mode is regulatory.
- **Legal exposure: HIGH.** SEC Release 33-11412 (March 17, 2026) explicitly names buybacks and burns as "market support activities" relevant to Howey analysis. The mechanism reinforces the "efforts of others" prong because the protocol is acting on behalf of tokenholders' price expectations.

3.5 Endowment / one-time payment for permanence

- **Definition:** users make a one-time payment in the native token at service entry; payment funds a permanent endowment that pays service providers over time.
- **Pioneer:** Arweave.
- **Demand:** upfront utility consumption.
- **Supply sink:** permanent lock in the endowment; paid out over time.
- **Failure mode:** failure to model real cost decline (Kryder's-law assumption); endowment underfunds long-tail service.
- **Legal exposure:** Low. One-time service payment is the cleanest "consumptive" pattern. Arweave has not drawn enforcement. Closest to "digital tool" in the 2026 SEC five-bucket taxonomy.

3.6 Pure governance with foundation split

- **Definition:** token's only utility is voting; explicit two-entity structure separates the DAO (token-governed, no commercial operations) from the operating entity (commercial, runs the protocol products).
- **Pioneer:** Ondo. Lido is the negative example — Lido did NOT split structurally, and the Samuels ruling exposed LDO holders to general-partnership liability.
- **Demand:** governance utility only.
- **Supply sink:** none direct; voluntary lockup possible.
- **Failure mode:** weak token-value link → speculative-only pricing → tokenholders don't actually govern (apathy).
- **Legal exposure:** Counterintuitive. Looks safest (no fee claim) but Samuels v. Lido DAO created general-partnership liability that's independent of securities law. **The Foundation/Operations split is the explicit defensive structure Ondo built to mitigate this; Lido lacked it.**

---

4. Legal framing — the March 2026 SEC interpretation

The SEC issued **Release 33-11412 on March 17, 2026** (the Atkins-era interpretive release), superseding the 2019 framework. Key elements:

- **Five-bucket taxonomy:** digital commodities, collectibles, tools, stablecoins, digital securities.
- **Howey narrowed:** "expectation of profits" anchored to **issuer promises at offering** rather than secondary-market trading. Pure secondary-market price appreciation alone is no longer dispositive.
- **Buybacks and burns explicitly named as Howey signals:** they are "market support activities" that reinforce the "efforts of others" prong even absent explicit promises.
- **Effort tracing:** LBRY-style "retention of supply signals motivation to increase value" remains relevant.

4.1 Case precedents that frame the design space

- **SEC v. Telegram (SDNY 2020):** $1.7B pre-sale of Gram purchase agreements was an unregistered offering. The court treated the SAFT pre-sale + anticipated public distribution as a "single scheme" / "disguised public offering." **Pre-sale + public distribution = high risk.**
- **SEC v. Kik (SDNY 2020):** consumptive utility did NOT save Kin; pre-sale and TDE treated as "single integrated offering." **Consumptive utility is not a shield if the issuer promotes profit potential.**
- **SEC v. Coinbase staking (June 2023; dropped Feb 2025):** the "pooled staking" theory; March 2024 motion-to-dismiss denial showed the SEC's theory was non-frivolous. **Dismissed without adjudication** — the theory survives in dormancy.
- **SEC v. LBRY (Nov 2022):** retention of LBC supply signaled motivation to increase value, supporting Howey finding even absent explicit profit promises.
- **SEC v. Ripple (July 2023):** $728M institutional sales were investment contracts; programmatic exchange sales were not. **The "no privity / no expectation tied to issuer" carve-out for programmatic sales remains controversial but live.**
- **SEC v. Binance (June 2023; dropped May 2025):** BNB's quarterly buyback/auto-burn was charged as unregistered security feature. **Dropped without adjudication.**

4.2 The Lido general-partnership ruling

- **Samuels v. Lido DAO (SDNY 2023; survived motion to dismiss Nov 2024):** Lido DAO treated as a general partnership; LDO holders potentially personally liable for DAO operations.
- **Implication:** pure-governance tokens without a Foundation/Operations split do not escape liability — they may aggregate it onto holders directly. **This is independent of federal securities law.**
- **Defensive structure:** Ondo's two-entity split (Foundation vs Ondo Finance Inc., with explicit "no ownership / no revenue rights" disclaimer) is the explicit mitigation.

4.3 MiCA (EU)

- **Recital 22:** services provided "in a fully decentralised manner, without intermediaries" are exempt — but the operative text has NO formal definition.
- **ESMA treatment:** decentralization is a spectrum, case-by-case, focused on control (admin keys, upgrade authority, voting concentration, official frontends).
- **Implication:** any token-controlling DAO with active multisig admin keys or substantial voting concentration faces MiCA scrutiny. Hyperliquid's Foundation Delegation Program's explicit US/Ontario exclusion is the kind of structural firewall that helps; Lido-style "DAO controls everything but is also the legal entity" does not.

4.4 2025-2026 enforcement shift caveat

- Coinbase, Binance, and Kraken-related dismissals in 2025 were **without adjudication**. The legal theories survive in dormancy.
- A future administration can reverse the 2026 SEC interpretation.
- State actions (California DFPI, NY OAG) continue independently.
- The Samuels v. Lido theory exists outside the SEC entirely.

Plain reading: the 2025-2026 enforcement environment is permissive relative to 2022-2024, but the legal theories that defined that earlier period are not dead — they are paused. A protocol design that relies on the current enforcement posture not changing is taking a risk on political continuity.

---

5. Nightshade-specific design options

Each option maps a primitive (or primitives) onto Nightshade's actual architecture: centralized v1 mint authority issuing blind credentials, 0.027182 XMR mint fee with 5000 XMR cap, 3-of-5 replica quorum, agent-to-agent payments on Monero per spec §33, marketplace per D-009, §22 session-binding handshake.

For each option: what it does, demand driver, supply sink, privacy interaction, legal risk profile, failure mode.

5.1 Option A — Replica/Mint Infrastructure Bond (Filecoin-style utility)

What it does: replica operators and the mint authority bond N tokens to participate in the 3-of-5 quorum / sign blinded credentials. Slashable for provable misbehavior (signing divergent snapshots per §19.3 transparency log; refusing valid registrations per §17.6 idempotency). Mint authority bond is larger than replica bonds, reflecting its higher trust position.

- **Demand:** dev plan §14.6 requires ≥5 replicas at v1 launch (2 team + 3 external per the Q4 resolution). Every replica operator is a structural buyer.
- **Supply sink:** bonded tokens locked while operating; ~6-month unbond period after exit.

- **Privacy:** bond happens at the operator layer (publicly-known replicas), NOT at the user-payment layer. Zero handshake interaction. Zero linkability between token holdings and operator identity beyond what the protocol already discloses.
- **Legal:** strongest Howey-defense profile in this list. Token's purpose is to acquire the right to operate; service-provider collateralization. Filecoin's SP collateral has not drawn SEC enforcement.
- **Failure mode:** thin operator set + concentrated token = capture risk. The 24-validator Hyperliquid cap is the design upper-bound; we target 5-15.

5.2 Option B — Burn-and-Mint Marketplace Credits (Helium HNT/DC redux, HIP-138 lessons baked in)

What it does: token is burned to mint non-transferable "Service Credits" pegged at a fixed XMR price. Credits pay for marketplace-layer features ONLY: discovery, listing priority, capability schema deployment, dispute escalation. **The underlying agent service payment stays on Monero per §33 — the token does NOT replace XMR as the agent-payment currency.** Emissions to replica operators + first-party reference agents calibrated against burn rate with sunset clause if burn doesn't reach threshold.

- **Demand:** marketplace consumption directly drives burn — each capability listing, discovery query, schema deployment burns tokens.
- **Supply sink:** burn-per-unit-consumption.
- **Privacy:** marketplace-layer interactions are already application-layer (visible); token burn at marketplace layer doesn't add linkability that wasn't already there. **Critical constraint: token must NOT touch §22 handshake or §33 service payment.**
- **Legal:** strong utility framing. Burn-and-mint is moderate exposure; Helium has not drawn enforcement.
- **Failure mode:** marketplace activity too low at launch → HIP-138's inflation trap. Mitigation: hard-cap bootstrap emissions; sunset clause; HIP-138-style "kill the subDAO" governance ability.

5.3 Option C — Endowment for Post-Cap Registration (Arweave-style)

What it does: simultaneously solves the design-pending §17.10 post-cap admission control question. Once the 5000-XMR cap is reached, new agent registrations require burning N tokens. Burns fund a programmatic endowment that pays replica operators + mint subsidies + reference-agent grants over time.

- **Demand:** post-cap registration is the entire demand driver. Pre-cap: registration is XMR; post-cap: registration is token.
- **Supply sink:** permanent lock in the endowment; paid out over time.
- **Privacy:** registration is the same already-known event with blind-credential unlinkability from XMR payment; token burn at registration doesn't add new linkability.
- **Legal:** one-time payment for clearly-consumptive service. Closest to "digital tool" in the 2026 SEC five-bucket taxonomy. Arweave has not drawn enforcement.

- **Failure mode:** only matters post-cap. If the cap is never reached, the token has no demand. Requires the early-XMR phase to actually succeed. Endowment solvency depends on a cost-decline model for replica/mint operations — analogous to Arweave's Kryder's-law assumption.

5.4 Option D — Pure Governance + Foundation Split (Ondo pattern)

What it does: two-entity structure — **Nightshade Foundation** (DAO governing protocol parameters, auditor pinning per spec §21, replica set composition, SDK release approval, post-cap admission policy) vs **Nightshade Operations** (commercial entity running the mint authority + reference agents + marketplace). Token governs the Foundation. Token explicitly disclaims any ownership, revenue rights, or claim on registration fees in Operations.

- **Demand:** pure governance utility.
- **Supply sink:** none direct. Voluntary lockup (vote-escrow style) optional.
- **Privacy:** metagovernance layer; zero user-flow interaction.
- **Legal:** most defensible STRUCTURE despite weakest demand. The Foundation/Operations split is the explicit Lido-Samuels mitigation. Critical: the structure must be REAL — Operations must have actual independent commercial agency.
- **Failure mode:** no structural demand → speculative-only price → tokenholder apathy. The Ondo DAO has passed ~9 proposals total; 100M ONDO required to submit one. A pure-governance Nightshade token may face the same apathy.

5.5 Option E — Hybrid: Bond + Marketplace Credits (single token)

What it does: single token serves both Option A and Option B. Replicas + mint bond it for operating rights; consumers burn it for marketplace features. Emissions calibrated to balance bond-locked supply, marketplace burn, and operator rewards.

- **Demand:** two structural demand layers — operators must acquire to operate; consumers must burn to use marketplace features.
- **Supply sink:** bonded (operator layer) + burned (consumer layer).
- **Privacy:** bond at operator layer; burn at marketplace layer; neither touches user-payment flow.
- **Legal:** utility-heavy, no fee distribution to passive holders, no buyback. **My recommended option on legal-defense grounds.**
- **Failure mode:** calibration is harder with two demand drivers; mistakes propagate.

5.6 Options I deliberately did NOT include

- **Buyback-and-burn from mint fees** (the current PROJECT_OVERVIEW §7 "15% buybacks" framing) — explicit Howey signal under SEC Release 33-11412. Direct correspondence with the dYdX v4 mechanism flagged as the most securities-like in the sample. **The existing §7 framing should be reworded or removed before any public token launch.**

- **Direct fee routing to stakers** (dYdX v4 pattern) — explicit Howey pattern.
- **Vote-escrow with fee accrual to lockers** (Curve/Pendle/Frax) — works for DEX-style protocols with high TVL but Nightshade has no comparable pool. The mechanism doesn't fit our architecture.
- **Algorithmic stablecoin** (Frax v1/v2 pattern) — Frax abandoned it; not relevant to Nightshade.
- **Yield tokenization** (Pendle) — no yield-bearing assets in Nightshade's domain.

---

6. Recommendation + the open strategic question

6.1 My recommendation, given the legal frame

Option E (Bond + Marketplace Credits, single token) as the cleanest demand-driven design with two structural supply sinks. Optionally layered with a Foundation-structure governance entity (Option D structure) if the opportunity requires a governance asset.

Specifically:

- Token utility is operator-layer (bond) + marketplace-layer (burn). Never user-payment-layer.
- Foundation/Operations split, regardless of governance scope, to mitigate Samuels v. Lido DAO general-partnership exposure.
- **Remove the "15% buybacks" framing from PROJECT_OVERVIEW §7** before any public communication. The current text is the single highest legal-attribution risk.
- Replace the "65% early holders" framing with utility-first allocation: bonded operator allocations + bootstrap emissions to marketplace + Foundation grants + team vesting. The "early holders" language is the Telegram/Kik trigger phrase.

6.2 The opportunity question

The token design space depends materially on what the opportunity is. The plausible categories shape mechanics:

1. **A specific exchange or launchpad listing** (Hyperliquid HIP-1? CEX? Solana launchpad?) — affects bridging, distribution mechanics, jurisdictional gating. Hyperliquid HIP-1 specifically would require ≥500 HYPE for the auction floor + HyperEVM bridging design + KYC-gated delegation considerations.
2. **An institutional partner or grant** (crypto-native VC, foundation grant, accelerator) — affects vesting, Foundation structure, accredited-investor pre-sale considerations (and the Telegram/Kik risk if pre-sale + public distribution).
3. **An infrastructure-incentive grant** (privacy-tech foundation, Monero community grant) — affects whether utility framing is the only viable mechanism (likely yes).
4. **A specific protocol integration** (cross-protocol composability, bridging requirement) — shapes the token's role around the integration's mechanics.

The Hyperliquid mention earlier hints the opportunity might involve their ecosystem. If so, that has specific implications worth fleshing out — HYPE-priced auction floor, native Hyperliquid spot market visibility, the KYC-gated Foundation Delegation Program excluding US/Ontario/sanctioned jurisdictions.

6.3 What I need from James to tighten the design

1. **What is the opportunity?** (CEX listing, launchpad, partner integration, grant program, etc.)
2. **Jurisdictional posture:** is US-investor access in scope, or are we excluding US (and accepting the corresponding distribution loss)? The Hyperliquid Foundation Delegation Program is the explicit model for US-exclusion.
3. **Counsel timeline:** when is counsel engagement happening? Token design without counsel signoff is exposure; the design above is a research-informed sketch, not a legally-cleared plan.
4. **PROJECT_OVERVIEW §7 rewrite:** the existing "65% early holders + 15% buybacks + 10% treasury" framing should be rewritten or removed before the opportunity becomes public. Independent of which option is chosen.

---

7. Primary source references

7.1 Hyperliquid

- HyperCore overview: https://hyperliquid.gitbook.io/hyperliquid-docs/hypercore/overview
- Staking: https://hyperliquid.gitbook.io/hyperliquid-docs/hypercore/staking
- HyperEVM: https://hyperliquid.gitbook.io/hyperliquid-docs/for-developers/hyperevm
- HIP-1: https://hyperliquid.gitbook.io/hyperliquid-docs/hyperliquid-improvement-proposals-hips/hip-1-native-token-standard
- HIP-2: https://hyperliquid.gitbook.io/hyperliquid-docs/hyperliquid-improvement-proposals-hips/hip-2-hyperliquidity
- HIP-3: https://hyperliquid.gitbook.io/hyperliquid-docs/hyperliquid-improvement-proposals-hips/hip-3-builder-deployed-perpetu
- Validator running: https://hyperliquid.gitbook.io/hyperliquid-docs/validators/running-a-validator
- Delegation program: https://hyperliquid.gitbook.io/hyperliquid-docs/validators/delegation-program
- Trading fees / AF: https://hyperliquid.gitbook.io/hyperliquid-docs/trading/fees
- Secondary (TGE, allocation, AF percentages): The Block (post/328631, post/341424); CoinSpeaker; XT.com Native Markets coverage; listing.help.

7.2 Comparative-scan protocols

- **Helium:** docs.helium.com/tokens/data-credit; HIP-138 issue (github.com/helium/HIP/issues/1120).

- **Filecoin:** spec.filecoin.io/systems/filecoin_mining/miner_collaterals/; docs.filecoin.io verified-deals + block-rewards; FIP-0080 (github.com/filecoin-project/FIPs/discussions/774).
- **Render:** renderfoundation.com/upgrade; Medium completion post; Messari overview.
- **Akash:** github.com/akash-network/discussions/147; akash.network/roadmap/aep-23; Cito research tokenomics guide.
- **Arweave:** permaweb-journal.arweave.net/article/storage-endowment-explained.html; docs.arweave.org/developers/development/overview.
- **GMX:** docs.gmx.io/docs/tokenomics/rewards/; gov.gmx.io proposal 4901.
- **Curve:** resources.curve.finance/vecrv/overview/; resources.curve.finance/vecrv/fee-collection-distribution/.
- **Lido:** docs.lido.fi/lido-dao/; blog.lido.fi/dual-governance-overview/.
- **Frax:** docs.frax.finance/; docs.frax.finance/fxs-and-vefxs/seigniorage.
- **Pendle:** docs.pendle.finance/ProtocolMechanics/Mechanisms/vePENDLE; docs.pendle.finance/ProtocolMechanics/Mechanisms/Fees.
- **dYdX v4:** docs.dydx.xyz/concepts/trading/rewards; dydx.foundation/blog/understanding-rewards-and-fees-on-the-dydx-chain.
- **Ondo:** docs.ondo.foundation/ondo-token; docs.ondo.foundation/ondo-dao; tokenomist.ai/ondo-finance.

7.3 Legal precedents

- SEC v. Telegram: Cooley client alert; WilmerHale client alert.
- SEC v. Kik: Jones Day analysis; Justia SEC v. Kik Doc. 88.
- SEC v. Coinbase staking: SEC press release 2023-102; SEC litigation release LR-25751 (dismissal).
- Kraken settlement: SEC press release 2023-25.
- SEC withdrawal pattern 2025: Sheppard Mullin whitecollarlawblog Feb 2025.
- SEC v. Ripple: Skadden publication.
- SEC v. LBRY: Greenberg Traurig insight.
- SEC v. Binance: SEC press release 2023-101; CNBC May 29, 2025 (dismissal).
- ESMA CA-as-FI guidelines (Dec 2024): esma.europa.eu Final Report.
- MiCA "fully decentralised" exemption: Aurum Law newsroom.
- Lido Samuels: blockchain.news class-action coverage.
- MiCA Liquid Staking: MiCA Crypto Alliance news.
- **SEC Release 33-11412 (March 17, 2026):** sec.gov/files/rules/interp/2026/33-11412.pdf.
- 2026 framework analysis: WilmerHale client alert March 24, 2026.

8. What this document is NOT

- A binding decision. No D-entry has been recorded; the recommendation in §6 is a research-informed sketch, not a counsel-cleared plan.
- Legal advice. Nothing here is legal advice. The §4 framing is research; the actual legal analysis requires counsel engagement.
- A finalized token design. Supply, allocation, vesting schedule, exact mechanics — all unspecified pending the opportunity question (§6.2).
- A response to the public-communication discipline. Per dev plan §15, any public token launch must be reviewed against the "Status, honestly" doctrine + the "no audited / production-ready / secure" constraints + the legal-pause from earlier this session (§4 + memory).

---

9. Open items this document surfaces

1. **The opportunity** that motivated the research — unspecified at time of writing. Design tightens once known.
2. **PROJECT_OVERVIEW.md §7 rewrite.** The current "65% early holders + 15% buybacks" framing should be rewritten before any token launch. Independent of which option in §5 is chosen.
3. **Counsel engagement timeline.** The §4 framing identifies the design constraints but does not substitute for actual legal review.
4. **Jurisdictional posture.** Excluding US (Hyperliquid model) trades distribution for liability mitigation; including US requires substantially more conservative design.
5. **Token name vs project name.** The Nightshade project name collides with U-Chicago's image-protection tool (per dev plan §17.9). Token naming inherits this constraint.
6. **The §17.10 post-cap admission control design.** Option C in §5 is a candidate solution; should be coordinated with the existing §17.10 design-pending status.
7. **Fee distribution missing 10%** (PROJECT_OVERVIEW §11). Any token launch is the natural moment to resolve this; the "missing 10%" can absorb whatever allocation the chosen token model requires.

This document is the research artifact for a future D-013-style decision on Nightshade tokenomics. It does not itself constitute that decision. The decision should be recorded in `DECISIONS.md` once the opportunity is concrete and counsel-reviewed.