



Master Brief

A complete reference for Coldstar — what it is, who's building it, where it stands, and what's next. Prepared as a knowledge source.

Coldstar in one line

Open-source, air-gapped signing infrastructure for Solana. Coldstar turns any USB drive into a cold wallet — no proprietary hardware. Private keys are encrypted at rest and decrypted only in locked memory for the microseconds it takes to sign, never written to disk in plaintext and never exposed to the network.

The thesis: hardware-grade self-custody shouldn't require buying a \$200 device. If the entire signing path is open source and the key never leaves an air gap, any USB drive is enough — for a person, a DAO treasury, or an autonomous AI agent.

WHAT COLDSTAR IS

- **Any USB → cold wallet.** Encrypted key storage on ordinary USB media; no vendor lock-in, no firmware you have to trust.
- **Air-gapped signing.** The signing machine never needs a network connection. Build the transaction online, cross the gap, sign offline, broadcast online.
- **Rust signing core.** Keys decrypted only in memory-locked (mLock) RAM, zeroized after use, cleaned up on panic — roughly microsecond key lifetime in memory.
- **Encryption:** AES-256-GCM for key encryption at rest; Argon2id passphrase stretching to resist brute force on a stolen drive.
- **Open source & auditable.** The full signing path is public — no black-box secure element to take on faith. "Verify me," not "trust me."
- **Cross-platform CLI.** macOS, Linux, Windows; Python 3.11+ and a USB drive, nothing else. Also ships as a Seeker (Solana Mobile) app.
- **Assets:** signs any SPL token, including tokenized real-world assets that live on Solana as SPL mints (e.g. PAXG gold, xStocks tokenized equities). Jupiter routing for swaps.

WHO WE ARE

Entity	ChainLabs Technologies — Surrey, UK
Founding Engineer	Ray (Rayyan) Akhtar — @devsyrem. Builds and ships the signer.
Product / GTM	Matthew Karsten — AI-agent / MCP background (Solana MCP, 1,000+ users); partnerships and go-to-market.
Advisor	Russ (Shiba / teamSHIB)
Brand	COLDSTAR wordmark + snowflake-in-shield mark. Black + circuit-trace, sci-fi identity.

What we’re building

PRODUCT SURFACE

- **Coldstar signer** — the CLI + Seeker app cold-signing core (shipped).
- **Swap** — best-price routing through Jupiter, with the signing step kept air-gapped. 1% platform fee, capped at \$10.
- **Bridge** — cross-asset movement.
- **Jito staking** — cold-signed SOL staking with Jito (on the roadmap; a dedicated flow alongside swap and bridge).
- **Agent-safe signing** — the wedge (see next section): give an autonomous agent the ability to transact without ever handing it a key.

Pricing

- **Free** — open-source CLI, any USB drive, standard 1% swap fee (capped \$10), community support.
- **\$39 (one-time)** — custom dual-connector (USB-A + USB-C) Coldstar drive, reduced swap fees, direct support.

THE WEDGE: AGENT-SAFE SIGNING

AI agents are starting to move real money on Solana. Most designs hand the agent a raw private key — one prompt injection empties the wallet. Coldstar is the **air-gapped root of trust** that lets an agent transact without owning the key.

The tension it solves

A true air gap needs something to carry each transaction across it; an autonomous agent can't wait for a human every time. Resolution: **the cold key signs the policy, not every transaction**. It authorizes a bounded envelope once — spend limits, allowlisted programs, time windows — and the agent then operates inside that envelope with a hot session key. The cold root is only touched to change the policy, approve a high-value action, or recover.

Three jobs, three places

- **Compute** — the agent runs in an attested TEE (e.g. Phala dstack), a server, or on the Seeker. It proposes; it never holds a key.
- **Custody** — keys live in Coldstar (air-gapped) or Seed Vault (Seeker secure element).
- **Authorization** — policy enforced on-chain via a multisig / policy account.

The seamlessness path maps to real, shipped Solana primitives: **Squads v4 spending limits** and the **Solana Foundation's Subscriptions & Allowances** (on-chain spend caps built for agents-within-a-budget); session keys with embedded limits; instant revocation; TEE attestation; and a drop-in signer for frameworks like Solana Agent Kit.

Where we are

- **\$COLD** — live utility token (Meteora, CoinGecko-listed); launched via EasyA Kickstart. Mint & freeze authority revoked.
- **coldstar.dev** — live marketing site, including a dedicated /agents page on agent-safe signing.
- **Seeker** — Coldstar app listed on the Solana dApp Store.
- **Security** — signing path is open source; a third-party audit is **in motion with Hashlock**. **Not yet independently audited** — stated plainly.
- **Ecosystem** — cohorts / community with EasyA, MonkeDAO, CastleDAO, Superteam Ireland & UK, Solana Mobile.
- **Social** — @buildcoldstar (product), building in public.

BUSINESS MODEL

- 1% swap fee, capped at \$10 (via Jupiter referral).
- \$39 one-time custom USB tier (reduced fees + support).
- Utility-first token; value accrues through fees / access as agent usage grows. No revenue-share.

WHAT'S NEXT (ROADMAP)

- **Base expansion** — a Base (Ethereum L2) version of the signer; Coldstar becomes multi-chain from a Solana core.
- **Jito staking** — ship the cold-signed staking flow.
- **Agent policy layer** — on-chain policy accounts, session-key delegation, and TEE attestation checks that make agent-safe signing seamless.
- **Audit completion** — finish the Hashlock review of the signing path.
- **Content surfaces** — branded evergreen tutorial / demo / explainer videos on subdomains (demo · intro · tutorial.coldstar.dev).

HONEST POSITIONING (DO NOT OVERSTATE)

- **Not yet third-party audited** — open source specifically so it can be reviewed; audit in motion.
- **No Coinbase / Crypto.com backing** — do not claim it.
- **RWAs** = "signs any SPL token, including RWA tokens" — not a bespoke RWA engine.
- **Solana-forward**, with Base as a deliberate expansion — not a scattered multi-chain claim.
- Air-gap protects the key, not the user's decisions or a compromised host OS; passphrase + backup discipline remain the user's responsibility.