

SpyON / SXP500 — Grant Reviewer Brief (v2, 11 September 2026)

Open-source Solana laboratory for a brokerless, fully collateralized synthetic exposure to the US large-cap reference. **Devnet and localnet only, valueless test assets, no mainnet, no real funds, not audited, not an ETF.** Public demo: <https://spyon-sxp500-demo.pages.dev> · Evidence: docs/DEVNET_EVIDENCE_2026-08-27.md and docs/DEVNET_EVIDENCE_2026-09-10.md

What it is

SXP is a synthetic token that follows the percentage move of the reference between two epoch prices. Two matched vaults (long principal vs. opposing liquidity) settle gains and losses on Solana; long principal can never exceed opposing collateral; returns are capped; a 0.25 % fee splits between treasury and insurance; an oracle adapter enforces freshness, confidence, monotonic time and a move breaker; a read-only guardian recommends pause. Route: TEST BTC → test USDC → SXP → (after settlement) test USDC → TEST BTC. Program EeCeb8mxJPVa1VotT6bn5N6upB8zLsv1vZFvgRPsuMHP (Anchor 1.1.2), Apache-2.0.

What changed since the 27 August brief

Item	Public proof (Solana Devnet, all <i>Finalized</i>)
Round trip closed (10 Sep, 23:36 UTC)	Epoch #1 settled and redeemed: oracle 5AUSRP...jh77, settle yi9ytF...SnJe, burn 0.153461538 SXP → 99.500625 test USDC 4kbMh1...mKhN, swap → 0.00152924 TEST BTC 25N5wP...QFqv. SXP mint supply for epoch #1 → 0. Net 100 → 99.500625 test USDC = 0.25 % in + 0.25 % out with the reference unchanged.
Tests re-run with date (10 Sep)	32 TypeScript + 5 Rust + 7 local-validator integration tests, all passing (Node 26.7, anchor-cli 1.1.2, solana-cli 3.1.10).
Reproducible build	anchor build from the public source package = sha256 8f95f667d8d5fe85ee588011d308efd56678d818b5b8f80193b58227d0c60ae, byte-identical to the program dumped from Devnet.
Epoch #2 + adversarial checks (10 Sep, 23:48–23:57 UTC)	Refusals recorded on-chain as failed transactions: insufficient opposing liquidity 52ty8z...zsp1, 2s27V7...HKmv (6022); stale oracle yXkBQB...RPak (6012); settlement before maturity 2cBvVV...eXNr (6019). Simultaneous claims from two wallets on the settled epoch: both succeed, vault conserved (5N9WMi...dNvPK, 3SaM6e...373Xe). Guardian: <i>pause-recommended</i> on a 146 s-old oracle, <i>healthy</i> after a fresh observation.
Separate test wallet	HVnCu2kEehZtwC9XPfskfLoL9mPfc1i4kv3c4YA3T2VB signs with its own key: swap 4x2R84...EeX4, mint 0.153461538 SXP 4xVfiK...JJx7, claim_short 3SaM6e...373Xe.
Web interface in Devnet mode (11 Sep, 00:14 UTC)	Reads program/epoch/pool/balances on-chain; the complete route was signed from the browser: swap 2XsQA2...Bh8j + mint 0.9965025 SXP mpQgZ7...93GV. A capacity-exceeding attempt was refused on-chain and surfaced verbatim in the UI.
Single canonical repository	Tag v0.5-devnet; version comparison in docs/VERSIUNI.ro.md; older tree kept as history.

Known limits (unchanged, stated plainly)

- **Oracle:** manual test observations signed by the configured authority. The Pyth/Hermes adapter and publisher exist and are unit-tested, but live SPY updates now require a Hermes API key (HTTP 401 without one, checked 11 Sep) and the Devnet instance was initialised with a documented test feed id; the official feed Equity.US.SPY/USD = 19e09bb8...1cd5 needs a fresh instance. This is Milestone 2 work.
- No independent audit, no legal opinion, no real BTC asset or bridge, no mainnet path. These are gates funded by the requested grant, not features.

- Admin, guardian and oracle authority are the same Devnet key (lab setup); key separation and multisig are pre-audit tasks.

How to verify in 15 minutes

1. Open any signature above on <https://explorer.solana.com/tx/<sig>?cluster=devnet>; failed ones show the AnchorError code in the log.
2. `solana program dump -u devnet EeCeb8mxJPVa1VotT6bn5N6upB8zLsv1vZFvgRPsuMHP prog.so && head -c 622800 prog.so | shasum -a 256 → 8f95f667...60ae`; then `anchor build` in the package and compare.
3. `npm ci && npm test && cargo test; anchor test --skip-build --validator legacy --provider.wallet target/local-admin.json` for the local-validator suite.
4. Read-only Devnet state: `node --import tsx scripts/devnet-inspect.ts` (needs any Devnet keypair as `ANCHOR_WALLET`, nothing is signed).

Ask

Milestone-based support (USD 45k equivalent, see [docs/funding/](#)): M1 independent reproduction + external-wallet evidence (largely done, see above), M2 verified oracle integration + adversarial suite, M3 independent audit + remediation, M4 legal and operational readiness. Founder contact and identity fields are completed privately before any submission.

Package integrity: the SHA-256 of the v2 source package is published next to it on the demo site. Private keys are never included. Prepared by the project's AI assistant on the founder's machine; every claim above links to on-chain data or to files in the package.