COLDSTAR

Air-gapped signing for the machine economy.

Hardware-grade key security, delivered as software. Live on Solana today — the signing layer for the agents that move money tomorrow.

$COLD · COLDSTAR.DEV · R[3]SIDENCY × CONSTRUCT 2026

Crypto almost never gets hacked. Keys do.

Nearly every major loss traces to one thing — a signing key that touched a machine it shouldn't have. This year, **Coldcard lost ~$70M** to a firmware bug that hid in open-source code for five years. The device was never the security. The air gap was.

~$70M
drained · Coldcard, 2026

128 → 32
bits of entropy · firmware bug

5 yrs
the flaw hid in open code

AI agents are about to move real money on Solana.

Autonomous trading, payments, and DeFi are here. But every agent architecture on the market assumes the agent is trustworthy — that's built for the demo, not production. The machine economy needs a signing primitive that **doesn't require blind trust in the software holding the keys.** None exists yet. That's the gap.

Air-gapped, policy-governed signing — as software.

- Any device becomes an air-gapped signer — **the key never meets the internet.**
- Fully open-source and verifiable — **read the code, don't trust the vendor.**
- Policy-governed signing built for agents, not just humans.

Today: humans — any USB + a Seeker. **Tomorrow:** the signing layer every agent calls before it moves a dollar.

The key and the internet are never in the same room.

ONLINE · UNTRUSTED

Everyday machine / agent host

Builds the unsigned transaction. Broadcasts the signed one. Never sees the key.

AIR GAP

OFFLINE · COLDSTAR SIGNER

The signer

Decrypts the key into mlock'd RAM, signs, zeroizes. No network, ever. Returns only the signature.

Rust · Argon2id + AES-256-GCM · key exposed ~100µs, wiped on panic · MIT, live on crates.io

Verify-me beats trust-me.

VS HARDWARE WALLETS

We delete the device

No $150 box, no factory, no firmware supply chain to trust. We reach the users Ledger and Coldcard price out — and can't be silently misconfigured.

VS HOT WALLETS

Air-gapped by design

Phantom, Backpack et al. keep the key on a networked device. Coldstar is offline from the ground up — the whole attack surface is gone.

VS MULTISIG / MPC

The open lane

No open-source, agent-native, air-gap-rooted signing primitive exists. That's the wedge — and where the machine economy is heading.

Shipped, live, and winning.

- **Live** on the Solana dApp Store
- **Open-source** core published on crates.io
- **$COLD** live — utility token, CoinGecko-listed
- **Partners:** EasyA · MonkeDAO · Triton One · Bit10 · SendAI
- **4×** Superteam Hackathon winner + Colosseum #62
- **Won** the Easy A Pitchathon
- **Hashlock** security audit in progress

Security builders who ship.

FOUNDER & TECHNICAL LEAD

Rayyan "Ray" Akhtar

@devsyrem

Architected and built Coldstar's air-gapped Rust signing core. Aerospace engineering background. 4× hackathon winner. Demoed Coldstar across Superteam and EasyA.

CO-FOUNDER · BUSINESS & TECHNICAL

Matthew Karsten

@expertvagabond

DevRel Engineer at ZetaChain (grew to 10k+ devs). Listing Manager at LBank ($5B+ volume). Solana MCP (1k+ users), 28 on-chain Anchor programs. Founder, Purple Squirrel Media.

The signing primitive for the machine economy.

Coldstar is crypto × AI, Solana-native, and building the exact infrastructure agents need to move money safely. With Construct's **$300K + 12 weeks**, we ship the agent-signing SDK, complete the Hashlock audit, and land mainnet integrations.

The vision: every agent that moves money on Solana signs through Coldstar.