We audit the math, not just the code.

A* Audit is a smart contract security firm focused on decentralized finance. We review DeFi protocols end-to-end, with particular depth on the math underneath — AMM curves, lending invariants, stablecoin pegs, derivative settlement, the places where small math errors compound into protocol-level failure. Our work begins with the invariants your system must hold, then asks whether they can be broken.

Where we work

Our practice covers DeFi protocols end-to-end:

- AMM and DEX architectures (concentrated liquidity, bonding curves, dynamic fees)
- Lending protocols (collateral systems, liquidation logic, interest rate models)
- CDP and stablecoin systems (peg mechanisms, governance, oracle dependencies)
- Derivatives (perpetuals, options, structured products — settlement, margin, risk parameters)
- Yield strategies and vaults with non-trivial economic invariants

For each, we cover the standard audit surface — access control, state transitions, integration boundaries — and go especially deep on the math that defines the protocol: curves, invariants, peg mechanics, settlement logic.

Methodology

Approach. First-principles and invariant-driven. We write down what your system must guarantee, then ask what could break those guarantees and how. The audit is manual review at its core, with formal reasoning applied where the math admits it.

Two angles, many questions. For every contract, we work along two axes: correctness under normal conditions, and resistance under adversarial ones. Within each, we probe the specific edge cases your protocol exposes. There is no fixed checklist, because every protocol breaks differently.

AI-assisted, human-led. We use AI tooling to accelerate code traversal, surface candidate issues, and pressure-test hypotheses. Every finding is then verified by a human auditor through manual review and critical reasoning. AI changes our speed, not our judgment.

Real-time delivery. Findings posted as labeled GitHub issues in your repository as the audit progresses — impact, likelihood, and status visible from day one. No black-box audit followed by a surprise document.

Team

thekmj (aka Catowice) — Co-founder & Lead auditor

Three-plus years auditing DeFi protocols across the full range — AMM, lending, CDP, perpetuals, yield. 7 first-place finishes and 12 top-3 placements across 42 contests, with results in every category audited: #2 on Arcadia Aerodrome (AMM), #3 on Perpetual (perpetuals), #1 solo on Napier V2 (yield, $47,408), #1 on predict.fun Lending. 22 validated High-severity vulnerabilities and $157,000+ in contest earnings across Sherlock, Cantina, Code4rena, CodeHawks, and Hats. Has also lead-judged 10+ audit contests — Jigsaw Finance, DESK Orderbook, and Peapods among them — evaluating findings submitted by other auditors and deciding which are valid. Senior Watson on Sherlock, Cantina Resident, Judge Overseer at Cantina. Repeat engagements with Blend Money and Arcadia Finance.

Supporting auditors. A team of 5–6 auditors with backgrounds in competitive mathematics and Solidity security. Every engagement runs under lead auditor direction.

Contact

Email · contact@astaraudit.com
Web · astaraudit.com