< Back to articles

Zunami Protocol audited by Ackee Blockchain

Andrea Nováková // AUDITS, ETHEREUM FEBRUARY 18, 2022

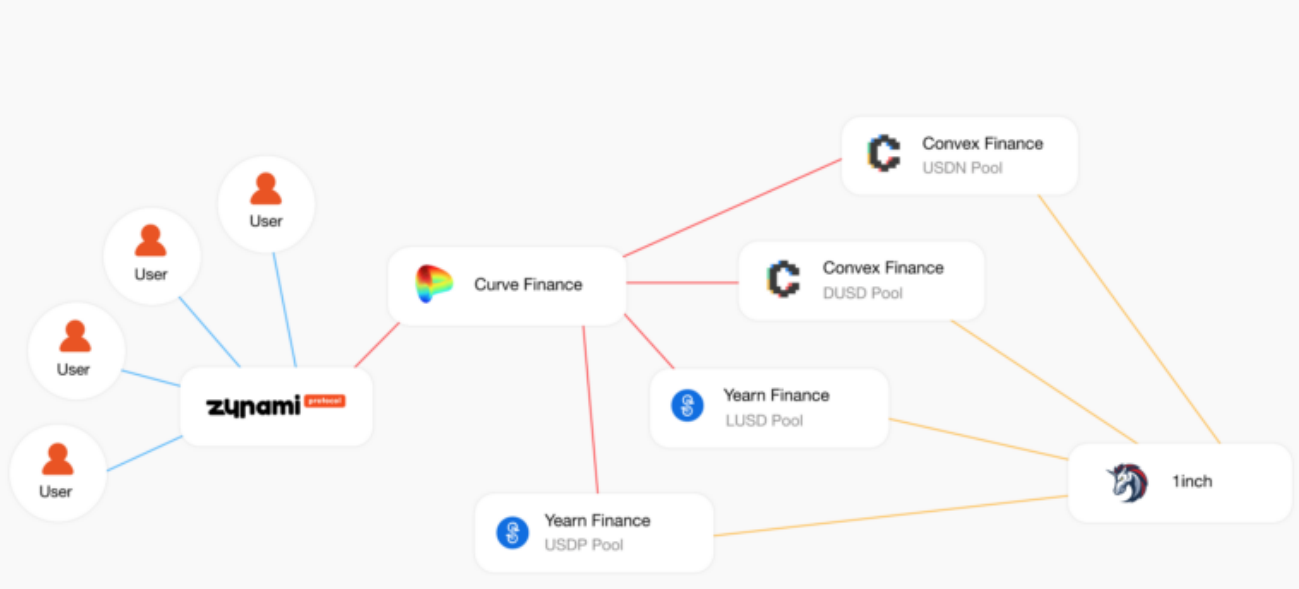
ABOUT ZUNAMI PROTOCOL

Update (18th August 2023): this audit report was performed on commit `37dccabf5aa3697dce5eaf6457debb3ac7404fdd`, the hack was performed by a donation (price manipulation) into strategy MimCurveStakeDAO (step 3) that was first added in

commit `6df0ae533a718a34df70984d745cc2d70fb7172d`, 28,296 additions ahead of this audit.

Zunami Protocol is **a multi-chain revenue aggregator for stablecoins** that generate profits within the existing market using risk-free assets.

It uses Transaction Streamlining Mechanism (TSM), reducing the commissions for individual transactions by **accumulating users' funds in one batch** and distributing it according to Zunami's strategies.



The Zunami Protocol **selects the most profitable strategies** by monitoring APY data and making calculations. Then, the users' funds are sent to Curve, and LP tokens are staked on Convex Finance or Yearn Finance.

Accumulated rewards in the DeFi protocol are automatically sold, and the profits are reinvested for the auto-compounding effect.

To learn more about the Zunami Protocol, read **the official documentation here**.

ABOUT THE AUDIT

Ackee Blockchain security team, engaged by Zunami Protocol, performed an audit of several contracts between **January 3 and January 14, 2022**. The entire audit process was conducted with a total time donation of **12 engineering days**.

At the beginning of the audit, the following **main objectives** were defined:

- Check the activity on the GitHub repository.

- Review the code quality, architecture, and best practices.
- Check for vulnerabilities if nobody can steal funds or damage contracts.
- Validate algorithms and math calculations for misbehaviors.
- Check if the contract's owner is not overpowered.

The audit methodology for Zunami Protocol consisted of:

1. **Technical specification/documentation** – a brief overview of the system is requested from the client, and the audit scope is defined.
2. **Tool-based analysis** – deep check with automated Solidity analysis tools is performed.
3. **Manual code review** – the code is checked line by line for common vulnerabilities, code duplication, best practices, and the code architecture is reviewed.
4. **Local deployment + hacking** – contracts are deployed locally, and we try to aack the system and break it.
5. **Unit testing** – run unit tests to ensure that the system works as expected. Potentially we write our unit tests for specific suspicious scenarios.

FINDINGS

Using the toolset, manual code review, and unit testing **led to the following findings**:

- L1: Inconsistent iteration statement syntax
- L2: Hardcoded token index
- L3: Confusing modifier naming
- M1: Unused virtual keyword
- M2: Public functions can be external
- M3: State variable could be local
- M4: Missing const
- M5: Unused variables
- M6: Code duplication
- M7: Interface issues

- M8: Unintended feature – Renounce ownership
- M9: Missing const
- H1: Management fee rewriting
- C1: Bug in the logic – wrong pool id
- C2: Rewriting deposit amounts

3 low severity, **9 medium** severity, **1 high** severity, and **2 critical** severity issues were identified.

CONCLUSION

Based on our audit report, the Zunami team responsibly took four weeks to resolve the audit findings.

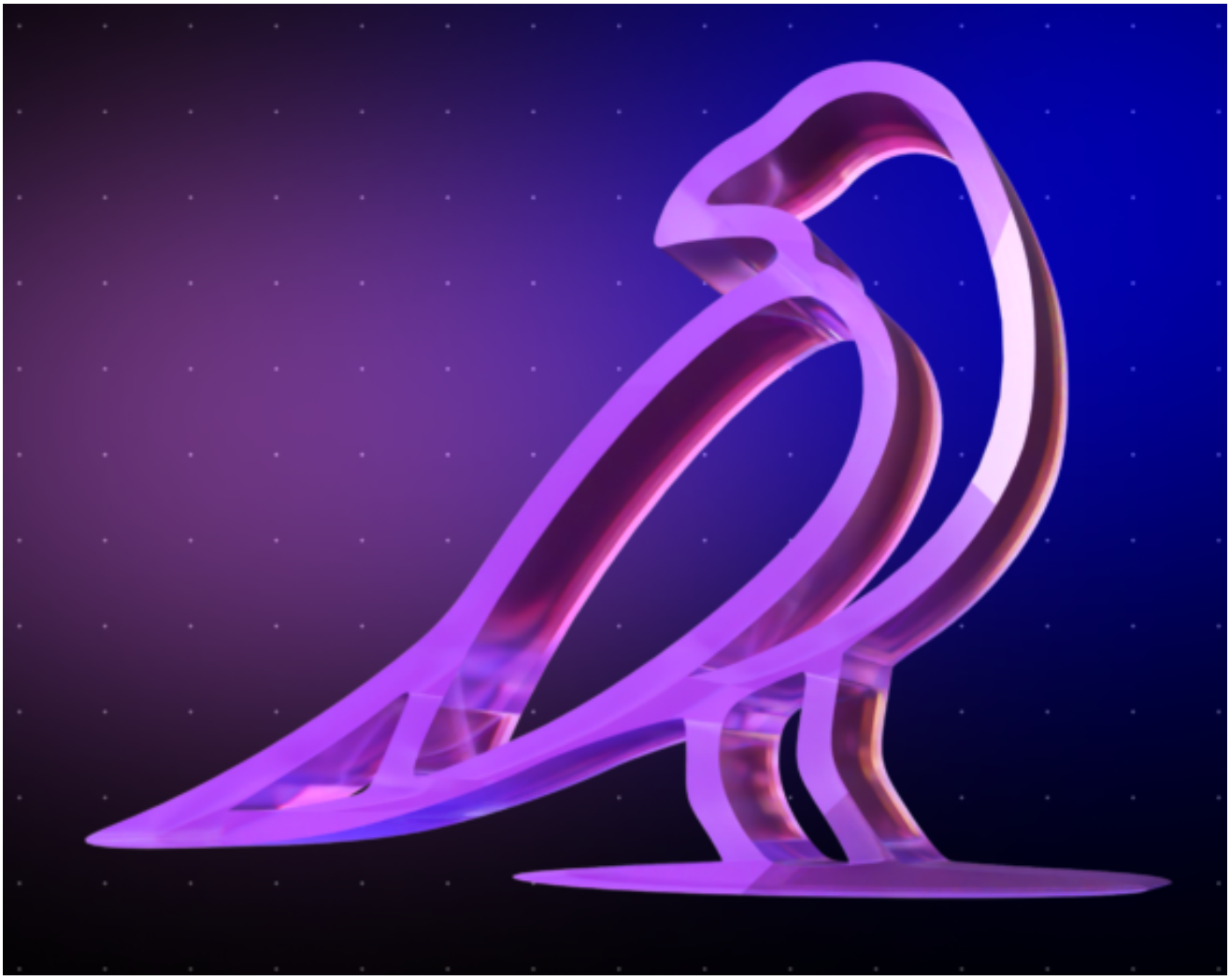
After the audit, we recommended a **re-audit**, which was performed between **February 16 and February 18, 2022**. In the re-audit, we reviewed whether all the findings have been fixed. The Zunami team **correctly fixed all issues** discovered in the first audit, and the codebase also improved between the two audit revisions. We found only one new minor issue.

We were delighted to audit the **Zunami protocol – a multi-chain revenue aggregator for stablecoins** and look forward to working with them again.

Audit Blockchain Cryptocurrency Ethereum Smart Contract Vulnerability Zunami.Protocol

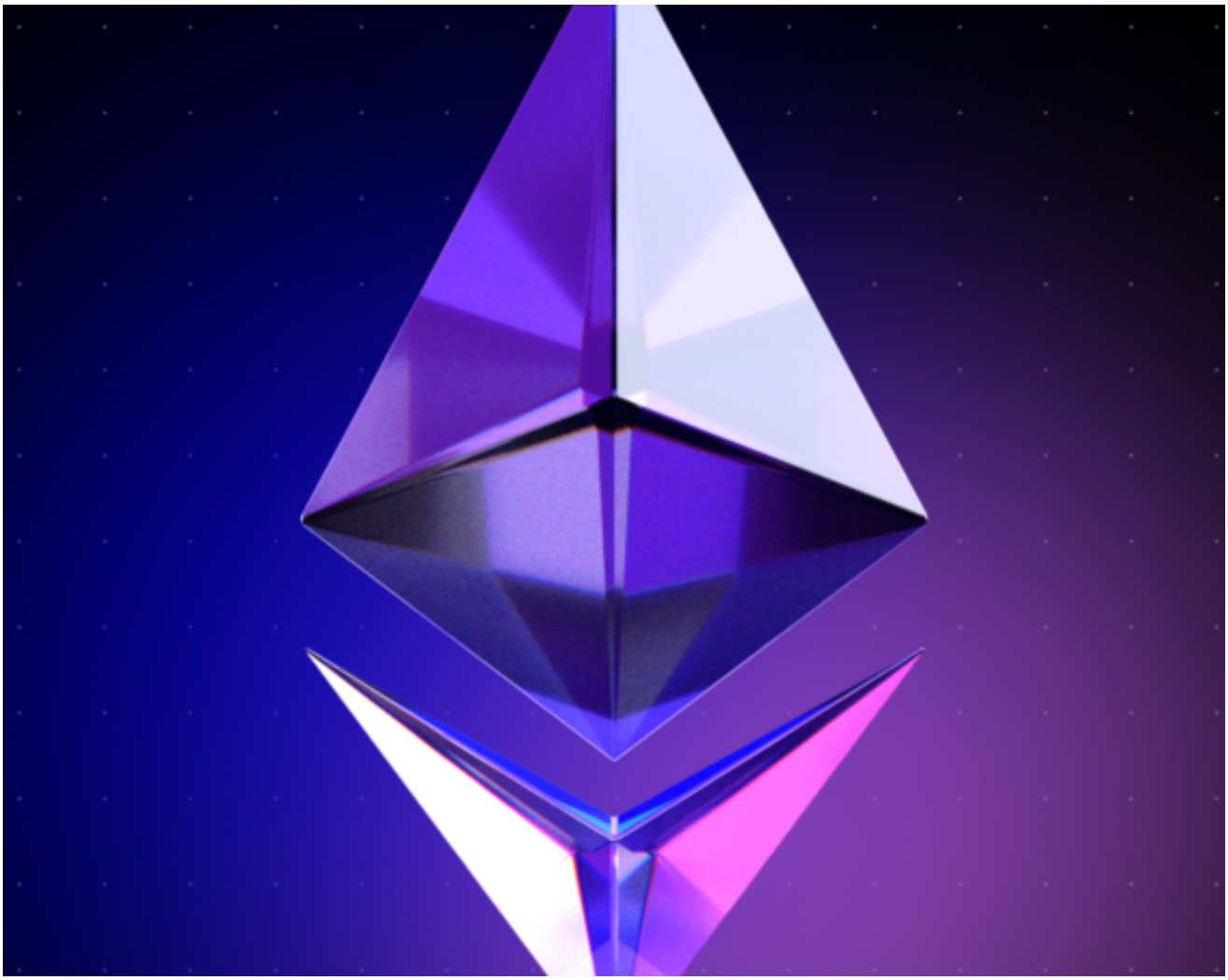
Andrea Nováková

You May Also Like



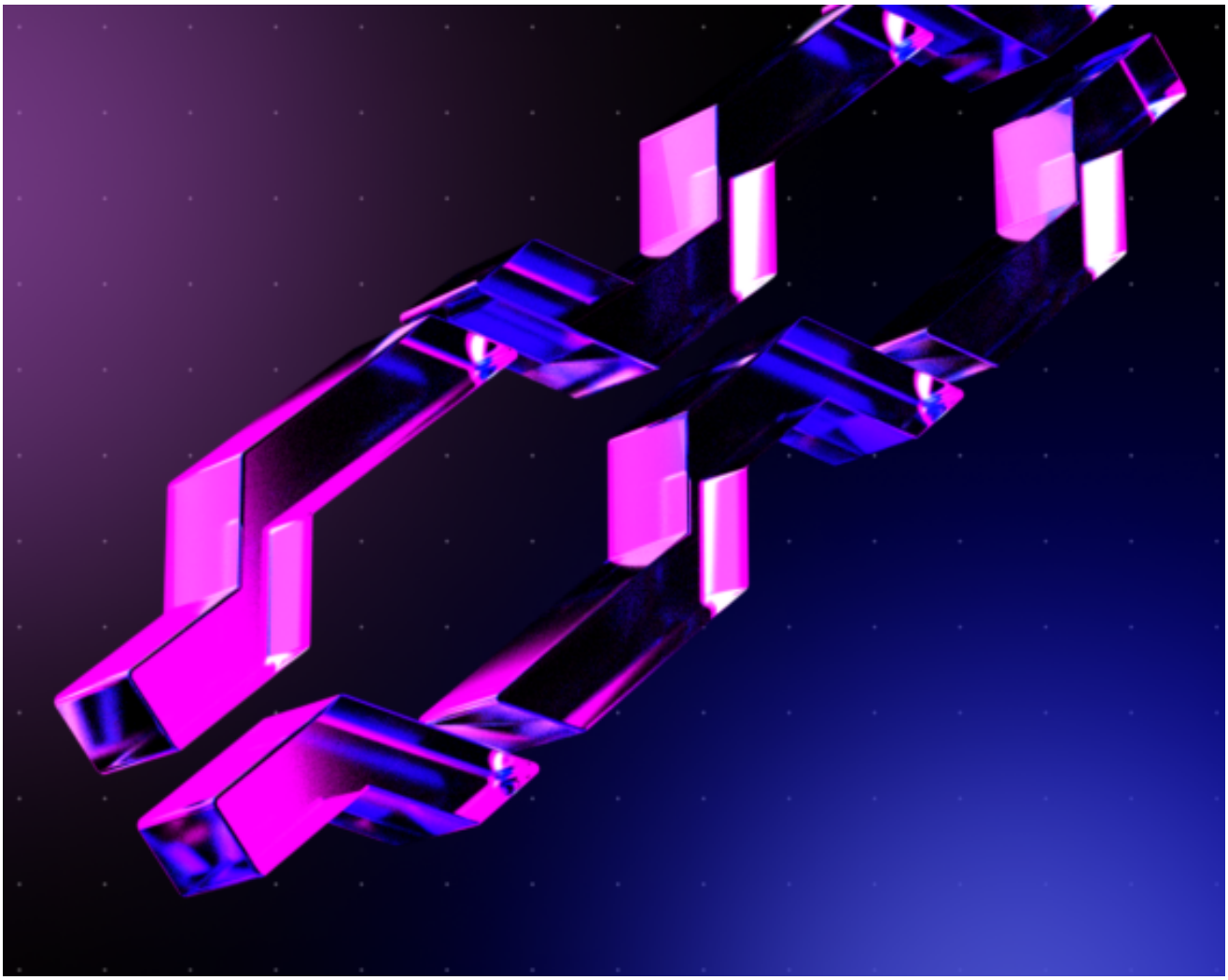
// AUDITS, ETHEREUM, SOLIDITY, WAKE MAY 14, 2025

VFAT Sickle Audit Summary



// EDUCATION, ETHEREUM APRIL 27, 2025

Ethereum's Pectra Upgrade: Security Implications and Insights



// EDUCATION, EXPLOITS, HACKS, SOLIDITY, WAKE APRIL 25, 2025

Reentrancy Attack in ERC-777