< Back to articles

Ackee Blockchain is an audit partner of 1inch Network

Andrea Nováková // AUDITS, ETHEREUM AUGUST 22, 2021

In 2021, Ackee Blockchain and 1inch agreed to **a long-term collaboration**.

1inch **adheres to the best security standards**, and before releasing any new feature or protocol enhancement, it is first reviewed **by five auditing companies**. All findings discovered by Ackee Blockchain were found on non-production code.

We, at Ackee Blockchain, are delighted to have partnered with 1inch and to be involved in auditing their future developments.

ABOUT 1INCH

1inch Network is **a DEX and DeFi aggregator protocol** across multiple chains. At the time of writing, 1Inch supports these blockchains: Ethereum, BSC, Polygon, Optimism, Arbitrum, Gnosis chain, and Avalanche.

How does 1inch work?

There are currently **3 protocols operating in the 1inch Network**: Aggregation Protocol, Liquidity Protocol, and Limit Order Protocol.

Aggregation Protocol

Aggregation Protocol provides **cost-efficient swap transactions** across multiple liquidity sources while offering competitive rates to users. 1inch incorporates the pathfinder algorithm that finds the best paths among different markets on supported blockchains.

Liquidity Protocol

Liquidity Protocol **allows users to earn passive income** on their crypto assets by depositing them in 1inch liquidity pools. The cryptocurrencies held in liquidity pools can then be used as the opposite side of transactions by traders who place trades using the 1inch decentralized exchange. In return, liquidity providers receive 'LP tokens' that can be staked or exchanged for other cryptocurrencies.

Limit Order Protocol

1inch limit order protocol is **a set of smart contracts** that can work on any EVM blockchain. Key features of the protocol are flexibility and high gas efficiency, which is achieved by using two different order types – regular Limit Order and RFQ Order.

In this blog post, we'll mention information about the following 1inch audits:

- **1inch Farming audit**
- **1inch Cumulative Merkle drop audit**
- **1inch Fixed Rate Swap audit** (the only one publicly accessible)

1inch Farming audit was performed between **January 27 and February 9, 2022**. Our security team found **2 low** severity issues. 1inch's development team fixed all findings.

1inch Cumulative Merkle drop audit was performed between **September 7 and September 10, 2021**. Our security team also found **2 low** severity issues that were fixed by 1inch's development team.

ABOUT THE 1INCH FIXED RATE SWAP AUDIT

The whole audit process consisted of **an audit and two re-audits**. Two auditors of Ackee Blockchain completed 1inch Fixed Rate Swap audit on **August 22, 2021**. The total time donation of this audit was **3 engineering days**, and the file being audited was *FixedRateSwap.sol (154 SLOC)*.

The first re-audit was completed on **November 18, 2021**, and the second re-audit was completed on **December 2, 2021**.

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

- Check the code quality, architecture and best practices.
- We should double check if mathematical algorithms are working as described, so there is no possibility of losing the funds due to mathematical error.
- Also it's important to ensure that nobody unauthorized can steal the funds held by the contract.
- Since the contract doesn't use a proxy upgrade pattern, we also need to focus on potential denial of service attacks.

We strive for a gradual and thorough approach to auditing the LayerZero protocol, which is why **our audit methodology consists of**:

1. **Technical specification/documentation** – a brief overview of the system is requested from the client, and the scope of the audit is defined.
2. **Tool-based analysis** – a basic check with automated Solidity analysis tools MythX and Slither is performed.

3. **Math validation** – mathematical calculations in the code are manually validated if results behave as defined.
4. **Manual code review** – the code is checked line by line for common vulnerabilities, code duplication, best practices, and the code architecture is reviewed.
5. **Local deployment + hacking** – the contracts are deployed locally, and we try to attack the system and break it.
6. **Unit testing and fuzzy testing** – additional unit tests are written in the Brownie testing framework to ensure that the system works as expected. Fuzzy testing is performed by Echidna.

FINDINGS

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

- L1: SWC-103 Floating pragma
- L2: Code duplicity
- M1: Potential token decimals mismatch
- M2: Unhandled division by zero – Zero and negative inputAmount is not handled before math operations
- H1: Unauthorized withdrawal

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

CONCLUSION

The overall **code quality is good**. Functions are well designed to avoid code duplicity. Executions of functions with invalid parameters are properly handled using require. However, the code isn't well documented; only the *getReturn()* function is commented, so we highly recommend covering all of the functions with documentation.

Based on our audit report, 1inch team responsibly took **several weeks to resolve the audit findings**. The 1inch's team **correctly fixed** all low and medium severity issues discovered in the audit, and the new 1inch Network feature invalided the high severity issue.

After the first re-audit, we were asked to re-validate the fixed code along with the newly implemented code in the first re-audit. During the second re-audit, we discovered just **one**

new minor issue.

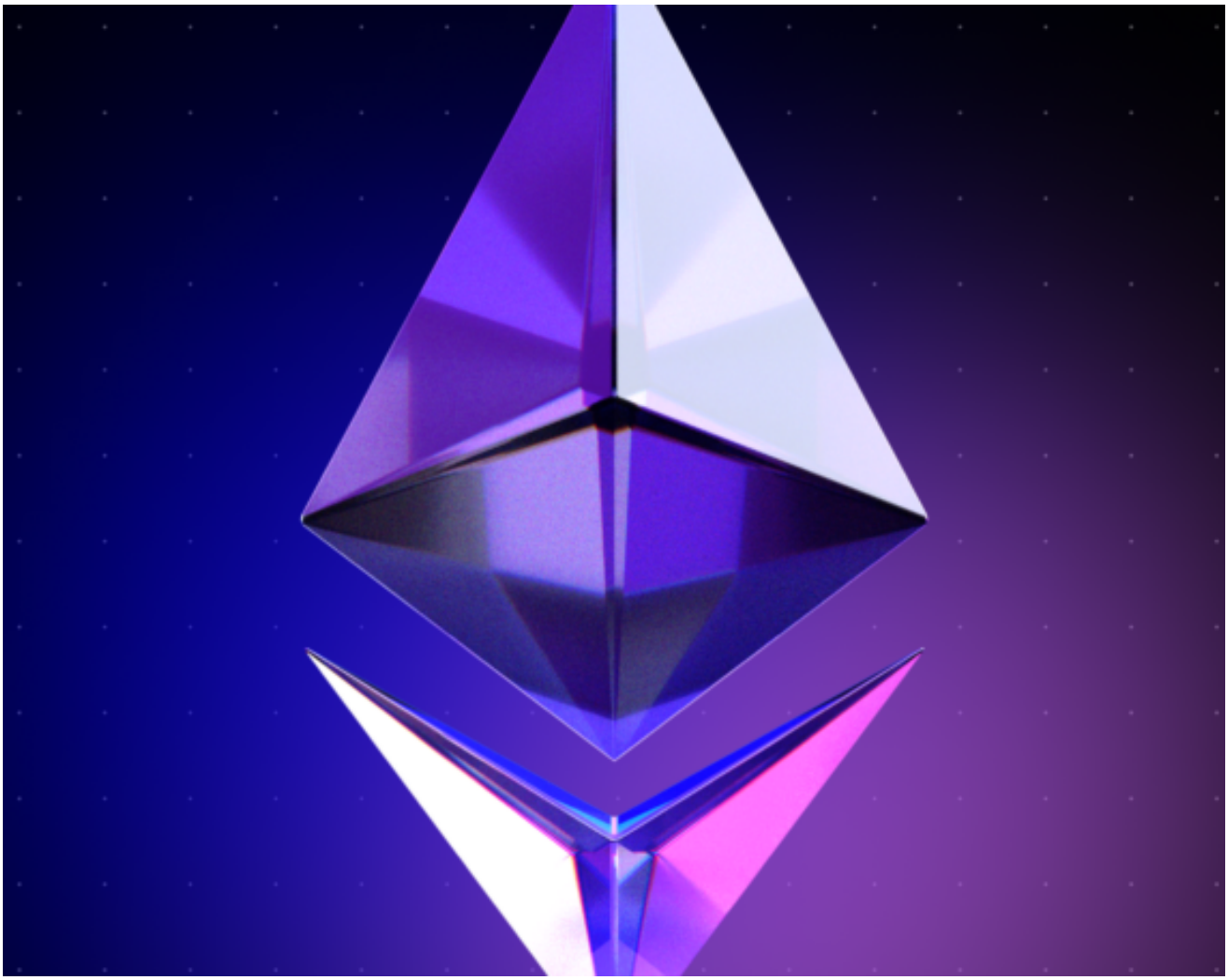
We were delighted to audit the **1inch Network** and we look forward to further cooperation.

The full Ackee Blockchain audit report of 1inch Fixed Rate Swap with a more detailed description of all findings and recommendations can be found here.

1Inch AMM Audit Blockchain Cryptocurrency DeFi Dex Ethereum EVM Vulnerability

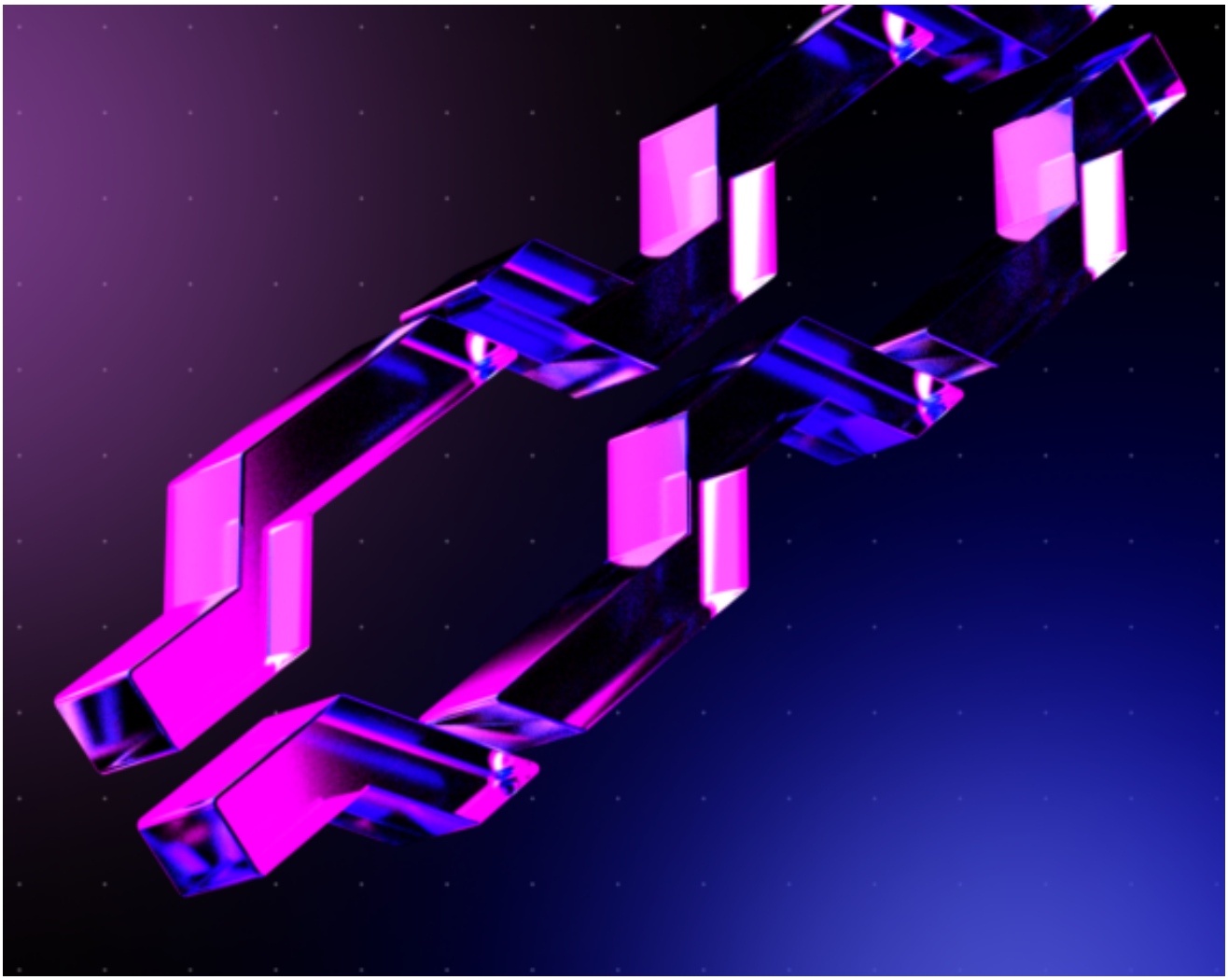
Andrea Nováková

You May Also Like



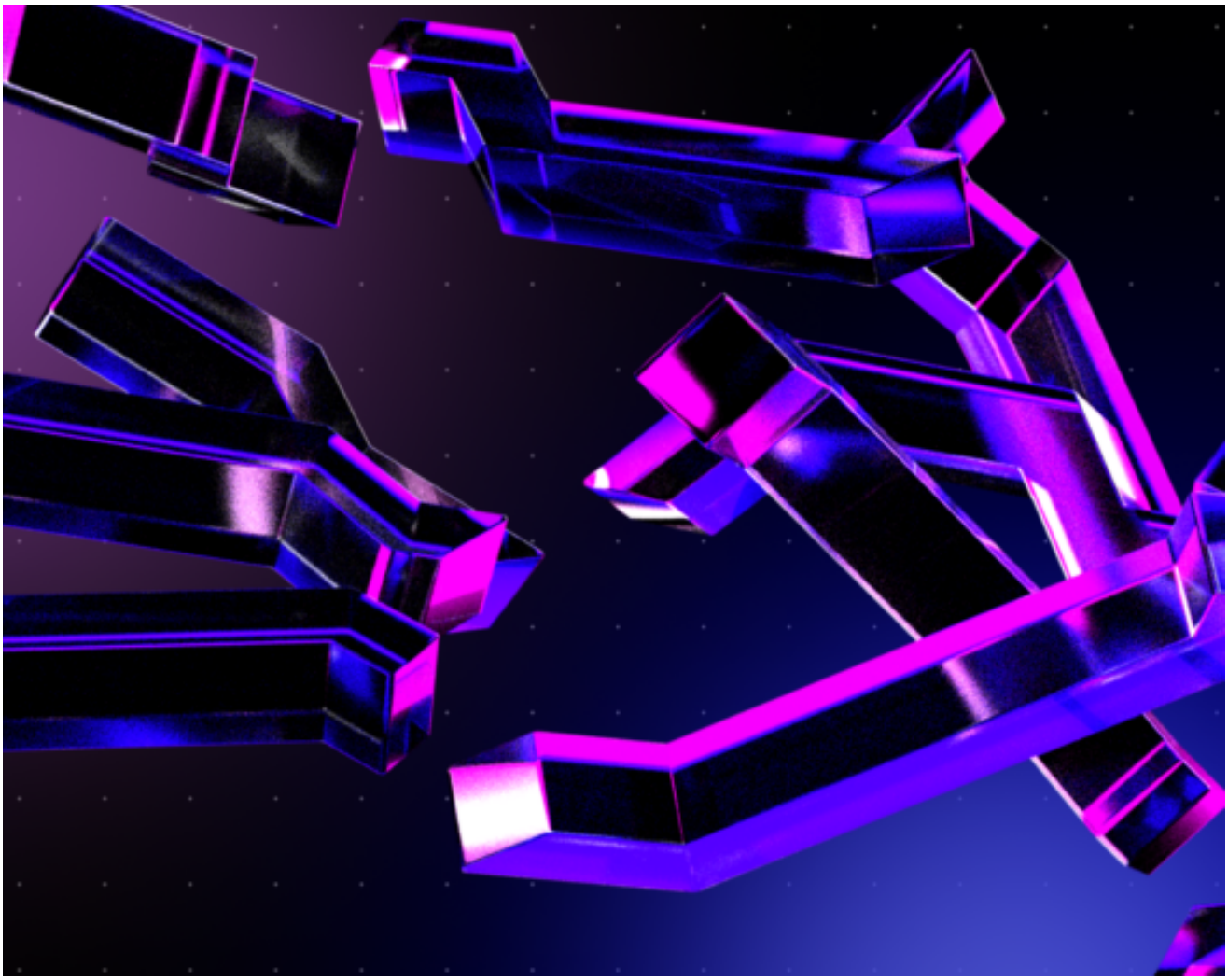
// EDUCATION, ETHEREUM APRIL 27, 2025

Ethereum's Pectra Upgrade: Security Implications and Insights



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

Reentrancy Attack in ERC-777



// EDUCATION, EXPLOITS, HACKS, SOLIDITY, WAKE APRIL 11, 2025

Flash Loan Reentrancy Attack