Unicrypt

Farms v2

SMART CONTRACT AUDIT

15.02.2022

Made in Germany by Chainsulting.de

Table of contents

1. Disclaimer

The audit makes no statements or warrantees about utility of the code, safety of the code, suitability of the business model, investment advice, endorsement of the platform or its products, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only.

The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, not to copy, disclose or disseminate without the agreement of SDD Tech OÜ. If you are not the intended receptor of this document, remember that any disclosure, copying or dissemination of it is forbidden.

Major Versions / Date	Description
0.1 (09.02.2022)	Layout
0.5 (11.02.2022)	Verify Claims and Test Deployment
0.6 (12.02.2022)	Testing SWC Checks
0.8 (12.02.2022)	Automated Security Testing Manual Security Testing
0.9 (14.02.2022)	Summary and Recommendation
1.0 (15.02.2022)	Final Document
1.1 (TBA)	Added deployed contract

2. About the Project and Company

Company address:

SDD Tech OÜ
Mustamäe tee 6b
Tallinn Harjumaa 10616

Website: https://unicrypt.network

Twitter: https://twitter.com/UNCX_token

Telegram: https://t.me/uncx_token

Medium: https://unicrypt.medium.com

2.1 Project Overview

UniCrypt is a decentralized services provider which offers several ways for DeFi projects to build community trust and keep users safe. Famously, UniCrypt created the first-ever liquidity locking smart contracts for Uniswap on Ethereum, known as Proof-of-Liquidity or POL. From there the project continued to develop new features, combining liquidity locking with a decentralized launchpad.

Liquidity Lockers: these are smart contracts that enable teams to publicly lock liquidity on Uniswap or other AMMs for a predetermined period. Essentially, it's a guarantee to investors that the project developers can't drain the pool of all the funds. A key innovation is UniCrypt's lockers will be able to migrate liquidity to Uniswap V3 when the time comes.

FaaS: This is a yield farming-as-a-service protocol that enables the creation of a farm for any token. Launch a farm in a couple clicks using the UI, all automatic with no coding necessary.

Launchpad: Perhaps the most interesting service, a 100% decentralized and automated presale platform that is connected to the liquidity lockers. Once the presale ends a portion of the raised funds (between 30% to 100%) will create the DEX pair on a supported AMM and the liquidity will be locked.

3. Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 – 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

4. Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

4.1 Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
   i. Review of the specifications, sources, and instructions provided to Chainsulting to make sure we understand the size, scope, and functionality of the smart contract.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Chainsulting describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
   ii. Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

4.2 Used Code from other Frameworks/Smart Contracts (direct imports)

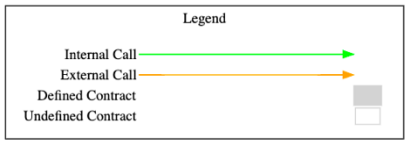
Dependency / Import Path	Source
Context.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v4.0.0/contracts/utils/Context.sol
EnumerableSet.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v4.0.0/contracts/utils/structs/EnumerableSet.sol
Ownable.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v4.0.0/contracts/access/Ownable.sol
ReentrancyGuard.sol	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v4.0.0/contracts/security/ReentrancyGuard.sol

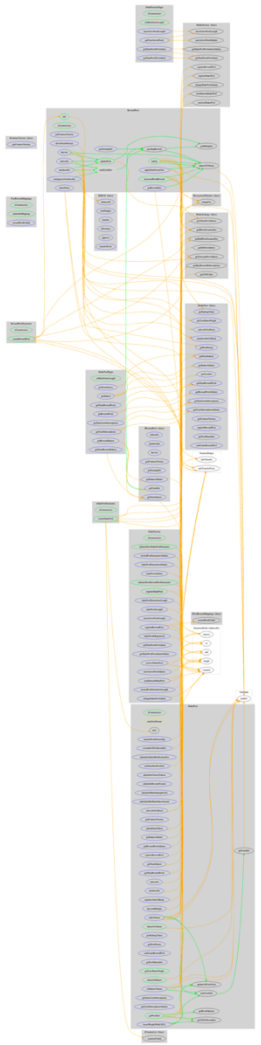
4.3 Tested Contract Files

The following are the MD5 hashes of the reviewed files. A file with a different MD5 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different MD5 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review

File	Fingerprint (MD5)
IStakeFactory.sol	a9b1606301109e648d55801c51b24b1d
IStakeSettings.sol	b9f1a9dfec87625d22e0baec9e8f08d6
PoolRewardMappings.sol	3d2eee4aa24d63c4e267eb7f5bb68e49
StakeFactory.sol	010859fe25682c08d3cb9cbf902c28a8
StakeSettings.sol	0d54a877587108a1a6154007cbc9680f
StakeFactoryPager.sol	e24de4c972986cc30dd80ca8d3c2e28c
IRewardPool.sol	a4e1500cc9eed227c1ccf8ea9d3667b5
StakePool.sol	e1cac740eb25aa6ab58dbcb7b92ddec5
StakePoolPager.sol	8077feb0280f2b8a4ec76bde5f645fd2
IEcosystemWhitelist.sol	fba8bd6123b89304d395cc2c74f08799
ICountryList.sol	442dfda2de615687a0ac89620eb34c58
RewardPoolGenerator.sol	56fd153761109aa22a195146b9aa5e02
RewardPool.sol	5d8a9ec04524640ece977c8f9997f921
IStakePool.sol	64a8e7be341f3c3b52eb92cf69d36895
IERC20.sol	7ad90e4c812fe07d426c8d955fcbabb4
StakePoolGenerator.sol	85f0b7e9e5fba0fb05939bb4a20534c8

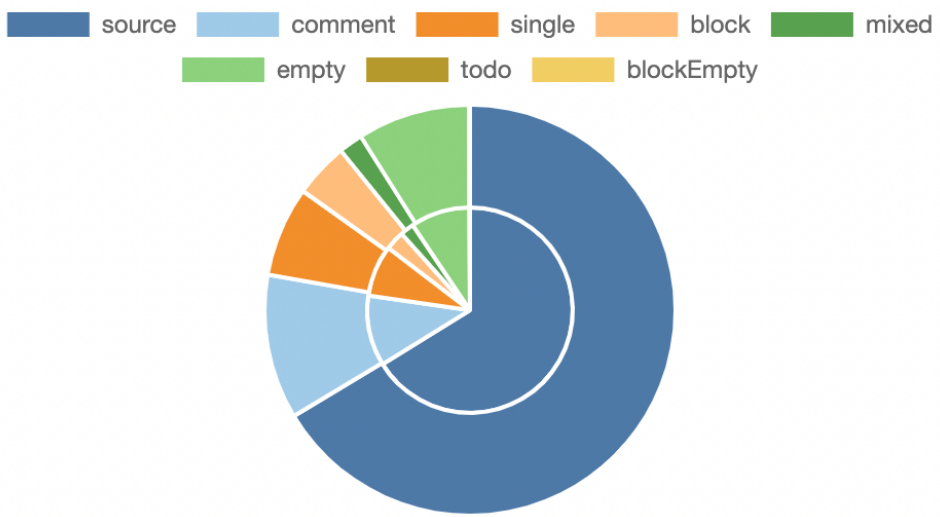
4.4 Metrics / CallGraph

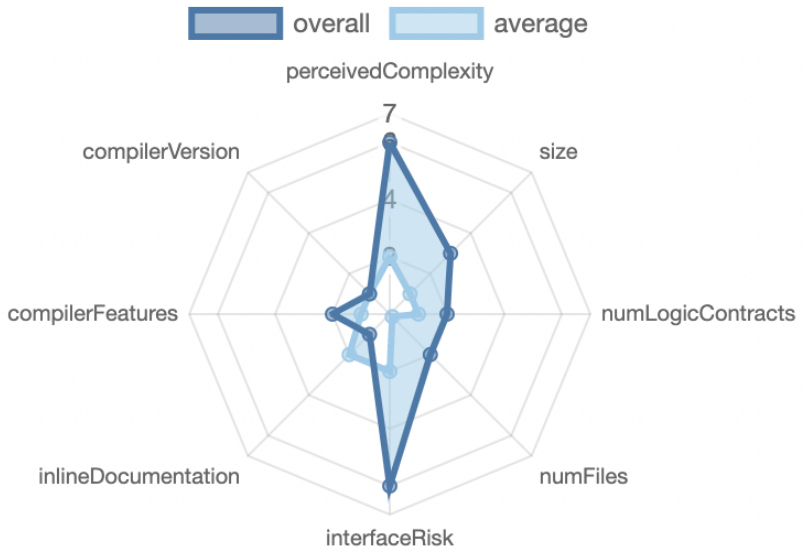




Full report: https://chainsulting.de/wp-content/uploads/2022/02/solidity-metrics-unicrypt-farmsv2.html

4.5 Metrics / Source Lines & Risk





4.6 Metrics / Capabilities

Solidity Versions observed	🧪 Experimental Features	💰 Can Receive Funds	🖥️ Uses Assembly	💣 Has Destroyable Contracts
`^0.8.0`		`yes`		

📪 Transfers ETH	⚡ Low-Level Calls	👥 DelegateCall	🧱 Uses Hash Functions	🪚 ECRecover	🌀 New/Create/Create2
`yes`					`yes` → `NewContract:RewardPool` → `NewContract:StakePool`

Exposed Functions
This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

🌐Public	💰Payable
157	4

External	Internal	Private	Pure	View
135	72	0	0	95

StateVariables

Total	🌐Public
41	31

4.7 Metrics / Source Unites in Scope

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
🔍	contracts/IStakeFactory.sol		1	20	9	3	4	19	
🔍	contracts/IStakeSettings.sol		1	16	9	3	4	15	
📝 🔍	contracts/PoolRewardMappings.sol	1	1	33	30	20	3	16	🔆
📝 🔍	contracts/StakeFactory.sol	1	2	222	168	118	27	109	🔆
📝	contracts/StakeSettings.sol	1		144	108	85	10	41	
📝	contracts/StakeFactoryPager.sol	1		72	72	50	12	56	
🔍	contracts/IRewardPool.sol		1	25	14	8	8	17	
📝	contracts/StakePool.sol	1		905	811	652	100	360	💰💾
📝	contracts/StakePoolPager.sol	1		140	140	97	29	103	
🔍	contracts/IEcosystemWhitelist.sol		1	10	9	3	4	3	🔆
🔍	contracts/ICountryList.sol		1	10	9	3	4	3	🔆

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
📝	contracts/RewardPoolGenerator.sol	1		98	89	76	5	41	🌀
📝	contracts/RewardPool.sol	1		569	536	453	47	195	
🔍	contracts/IStakePool.sol		1	51	27	20	15	33	
🔍	contracts/IERC20.sol		1	79	28	17	58	13	🔆
📝	contracts/StakePoolGenerator.sol	1		103	100	85	6	48	💰💠🌀
📝🔍	**Totals**	**9**	**10**	**2497**	**2159**	**1693**	**336**	**1072**	💰💠🌀🔆

Legend: [📝]

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

5. Scope of Work

The Unicrypt Team provided us with the files that needs to be tested. The scope of the audit are the Unicrypt Farms v2 contracts.

Following contracts with the direct imports has been tested:

- RewardPoolGenerator.sol
- StakeFactory.sol
- StakePoolGenerator.sol
- StakeSettings.sol
- PoolRewardMapping.sol
- StakePoolPager.sol
- StakeFactoryPager.sol

The team put forward the following assumptions regarding the security, usage of the contracts:

- The smart contract is coded according to the newest standards and in a secure way
- Checking the changes since the last audit https://github.com/chainsulting/Smart-Contract-Security-Audits/blob/master/Unicrypt/02_Smart%20Contract%20Audit%20Unicrypt_Farm.pdf

The main goal of this audit was to verify these claims. The auditors can provide additional feedback on the code upon the client's request.

5.1 Manual and Automated Vulnerability Test

CRITICAL ISSUES
During the audit, Chainsulting's experts found **no Critical issues** in the code of the smart contract.

HIGH ISSUES
During the audit, Chainsulting's experts found **no High issues** in the code of the smart contract.

MEDIUM ISSUES
During the audit, Chainsulting's experts found **no Medium issues** in the code of the smart contract.

LOW ISSUES

5.1.1 Hardcoded address
Severity: LOW
Status: ACKNOWLEDGED
Code: NA
File(s) affected: StakeSettings.sol

Attack / Description	Code Snippet	Result/Recommendation

The contract contains hardcoded addresses.	Line: 30
	`SETTINGS.UNCL_FEE_ADDRESS = payable(`
	`0x0da797beF1F3C234204aA3EF3A50a67B7aAeCB49`
	
	Line: 45
	`.UNICRYPT_DEV_ADDRESS =`
	`0xAA3d85aD9D128DFECb55424085754F6dFa643eb1;`
		Both addresses are known and most probably won't change in the future. Just in case they will change keep it as variable. In terms of Unicrypt Dev address we recommend a multisig wallet structure.

INFORMATIONAL ISSUES

5.1.2 OpenZeppelin libraries are not correctly imported
Severity: INFORMATIONAL
Status: ACKNOWLEDGED
Code: NA
File(s) affected: ALL

Attack / Description	Code Snippet	Result/Recommendation
In the current implementation, OpenZeppelin files are not correctly imported.	Context.sol, Ownable.sol, ReentrancyGuard.sol, EnumerableSet.sol	We highly recommend using npm (import "@openzeppelin/contracts/..) in order to guarantee that original OpenZeppelin contracts are used with no modifications. This also allows for any bug-fixes to be easily integrated into the codebase.

5.1.3 A floating pragma is set.
Severity: INFORMATIONAL
Status: ACKNOWLEDGED
Code: SWC-103
File(s) affected: ALL

Attack / Description	Code Snippet	Result/Recommendation
The current pragma Solidity directive is "^0.8.0". It is recommended to specify a fixed compiler version to	Line 1: `pragma solidity ^0.8.0;`	It is recommended to follow the latter example, as future compiler versions may handle certain language constructions in a way the developer did not foresee.

ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.		i.e. Pragma solidity 0.8.0 See SWC-103: https://swcregistry.io/docs/SWC-103

5.2. SWC Attacks

ID	Title	Relationships	Test Result
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code	✅
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	✅
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	✅
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	✅
SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	✅

ID	Title	Relationships	Test Result
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	✅
SWC-124	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	✅
SWC-123	Requirement Violation	CWE-573: Improper Following of Specification by Caller	✅
SWC-122	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	✅
SWC-121	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	✅
SWC-120	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	✅
SWC-119	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	✅
SWC-118	Incorrect Constructor Name	CWE-665: Improper Initialization	✅
SWC-117	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	✅

ID	Title	Relationships	Test Result
SWC-116	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	✅
SWC-115	Authorization through tx.origin	CWE-477: Use of Obsolete Function	✅
SWC-114	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	✅
SWC-113	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	✅
SWC-112	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	✅
SWC-111	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	✅
SWC-110	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	✅
SWC-109	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	✅
SWC-108	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	✅
SWC-107	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	✅

ID	Title	Relationships	Test Result
SWC-106	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	✅
SWC-105	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	✅
SWC-104	Unchecked Call Return Value	CWE-252: Unchecked Return Value	✅
SWC-103	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	X
SWC-102	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	✅
SWC-101	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	✅
SWC-100	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	✅

6. Executive Summary

Two (2) independent Chainsulting experts performed an unbiased and isolated audit of the smart contract codebase. The final debriefs took place on the February 16, 2022.

The main goal of the audit was to verify the claims regarding the security of the smart contract and the functions. During the audit, no critical issues were found after the manual and automated security testing and the claims been successfully verified.

7. Deployed Smart Contract

PENDING