MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

2021

UNICRYPT TOKEN PROGRESS REPORT

12 OCT 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

SUMMARY

This report has been prepared for Unicrypt smart contracts, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend add ressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

SECURITY ASSESMENT

BACKGROUND

MotechAudit was commissioned by Unicrypt to perform an audit of smart contracts:
https://etherscan.io/address/0xaDB2437e6F65682B85F814fBc12FeC0508A7B1D0
The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

SECURITY ASSESMENT

AUDIT DETAILS

AUDITED PROJECT

Unicrypt

DEPLOYER ADDRESS

0x60e2E1b2a317EdfC870b6Fc6886F69083FB2099a

CLIENT CONTACTS:

Unicrypt team

BLOCKCHAIN

ETHEREUM Project

WEBSITE:

https://unicrypt.network/

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and MotechAudit hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONTRACT DETAILS

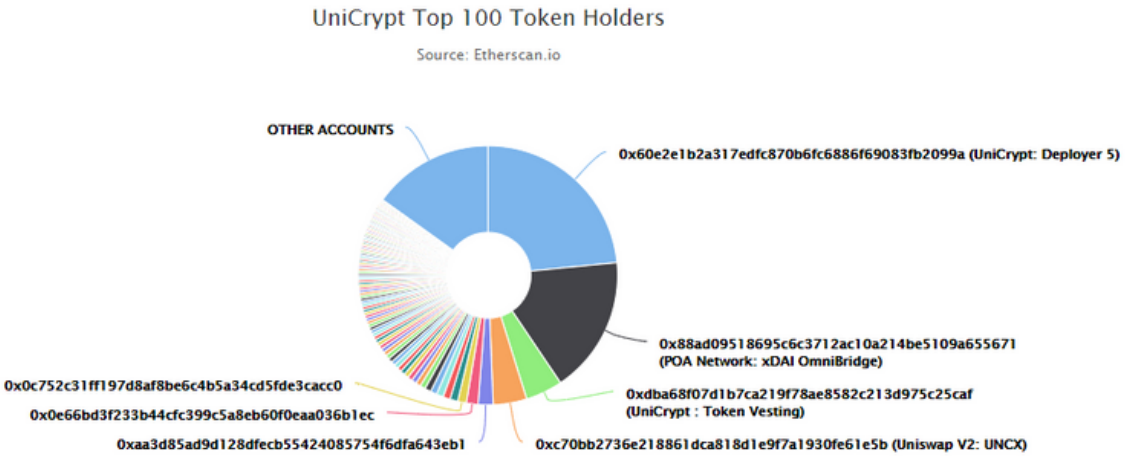
Token contract details for Oct-14-2020

Contract name	**Unicrypt**
Contract address	**0xaDB2437e6F65682B85F814fBc12FeC0508A7B1D0**
Total supply	**47,650**
Token ticker	**UniCrypt (UNCX)**
Decimals	**18**
Token holders	**2,088**
Transactions count	**41,359**
Top 100 holders dominance	**74.4301%**
Contract deployer address	**0x60e2E1b2a317EdfC870b6Fc6886F69083FB2099a**
Contract's current owner address	**0x60e2E1b2a317EdfC870b6Fc6886F69083FB2099a**

UNICRYPT TOKEN DISTRIBUTION

The top 100 holders collectively own 84.90% (40,456.70 Tokens) of UniCrypt

Token Total Supply: 47,650.00 Token | Total Token Holders: 2,088

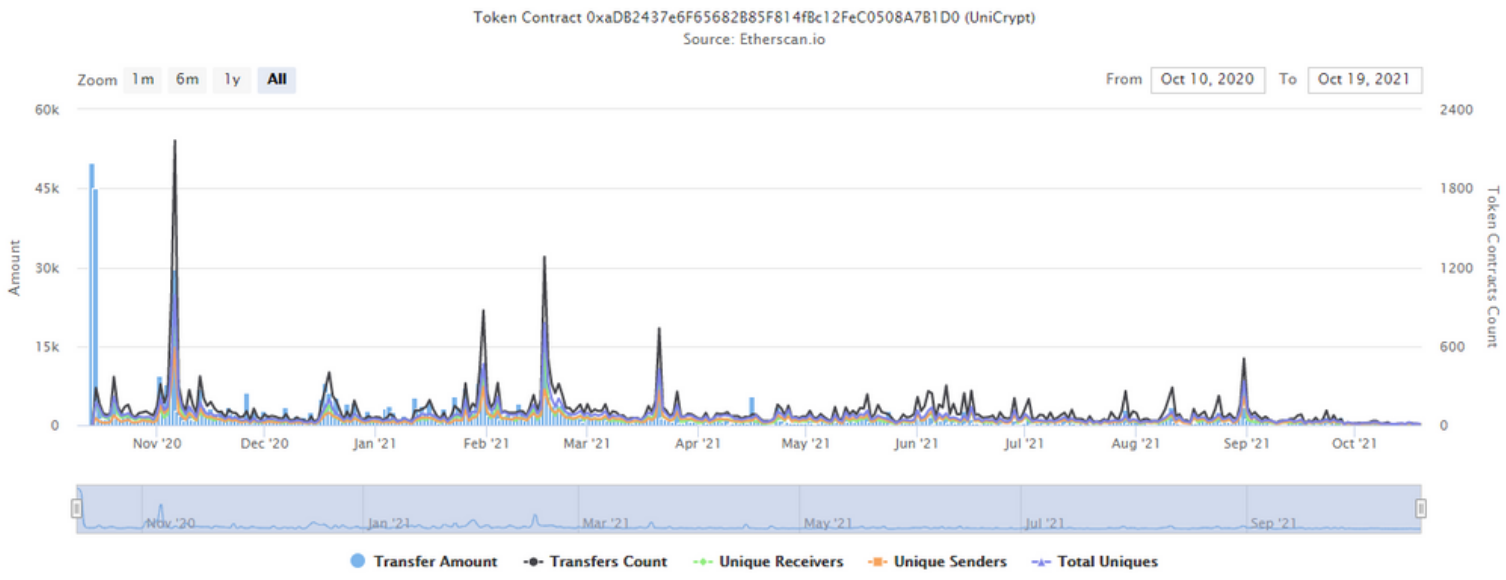


(A total of 40,456.70 tokens held by the top 100 accounts from the total supply of 47,650.00 token)

UNICRYPT TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Wed 14, Oct 2020 - Tue 19, Oct 2021



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	UniCrypt: Deployer 5	11,171.089025343702960362	23.4440%	$4,554,446.89	
2	POA Network: xDAI OmniBridge	8,155.79699633256693 5005	17.1160%	$3,325,113.98	
3	UniCrypt : Token Vesting	2,200	4.6170%	$896,938.80	
4	Uniswap V2: UNCX	1,995.276110978080005706	4.1874%	$813,472.98	
5	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	885.860881381839748382	1.8591%	$361,165.00	
6	0x0e66bd3f233b44cfc399c5a8eb60f0eaa036b1ec	700.01008937537401051	1.4691%	$285,393.73	
7	0x0c752c31ff197d8af8be6c4b5a34cd5fde3cacc0	515.636323463180299992	1.0821%	$210,224.65	
8	0xb7ea6b15b4cb4f7c978bc6b6f53237aef15659f5	460	0.9654%	$187,541.75	
9	0x016b6e1a9d05ac99b8f7bb5680a20e06489d43c1	429.283213260534249537	0.9009%	$175,018.53	
10	0x5869458f360d8c1ce49e35fccb3d0a1f25e8d533	418.52140393280905943	0.8783%	$170,630.95	

source:etherscan.io

SECURITY ASSESMENT

FINDINGS

Critical	0 (0.00%)
Major	0 (0.00%)
Medium	0 (0.00%)
Minor	2 (50.00%)
Informational	2 (50.00%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
MPV-01	Variable could be declared as `constant`	Gas Optimization	Informational	Resolved
MPV-02	Missing Emits Events	Coding Style	Informational	Resolved
MPV-03	Lack of Input Validation	Gas Optimization	Minor	Resolved
MPV-04	Lack of Input Validation	Gas Optimization	Minor	Acknowledged

SECURITY ASSESMENT

MPV-01 | VARIABLE COULD BE DECLARED AS CONSTANT

Category	Severity	Location	Status
Coding Style	Informational	Verifier.sol: 9	Acknowledged

Description

Variables that never changed after assignment, can be declared as constant.

- V1_LOCKER;
- V2_LOCKER;
- ALLOWED_SLIPPAGE

Recommendation

We recommend declaring those variables as constant.

Alleviation

[Unicrypt]: The team addressed the issues in the private repository.

SECURITY ASSESMENT

MPV-02 | MISSING EMITS EVENTS

Category	Severity	Location	Status
Coding Style	Informational	Verifier.sol: 9	Acknowledged

Description

The setSlippage() will modify the variable ALLOWED_SLIPPAGE. The missing event makes it difficult to the parameter changes. An event should be emitted for significant transactions as this.

Recommendation

We recommend emitting an event to log the update of onlyOwner in setSlippage.

Alleviation

[Unicrypt]: The team addressed the issues in the private repository.

SECURITY ASSESMENT

MPV-03 | LACK OF INPUT VALIDATION

Category	Severity	Location	Status
Coding Style	Informational	Verifier.sol: 9	Acknowledged

Description

In the setSlippage(), the input variable _slippage should sanitized with a given range of 5% or aboundary limit.

Recommendation

We recommend adding the range of the validation for _slippage.

```
55  function setSlippage(uint256 _slippage) external onlyOwner {
56        require(_slippage > 0 && _slippage<=5, "_slippage should be a value between 0 to
5")
57         ALLOWED_SLIPPAGE = _slippage;
58       }
59
```

Alleviation

[Unicrypt]: The team addressed the issues in the private repository. The value of ALLOWED_SLIPPAGE isnow required to be greater than 0% and less than or equal to 10% when setting a new value by callingfunction MigratePancakeV1.setSlippage().

SECURITY ASSESMENT

MPV-04 | LACK OF INPUT VALIDATION

Category	Severity	Location	Status
Coding Style	Informational	Verifier.sol: 9	Acknowledged

Description

In the setSlippageForToken(), the input variable _slippage should sanitized with a given range of 5 % ora boundary limit.

Recommendation

We recommend adding the range of the validation for _slippage.

```
59  function setSlippageForToken(address _lpToken, uint256 _slippage) external onlyOwner
{
60        require(_slippage > 0 && _slippage<=5, "_slippage should be a value between 0 to
5")
61          ...
62      }
63
```

Alleviation

N/A

Global Goals

CONCLUSION

Smart contracts contain owner privileges!

Motech Audit note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.