CERTIK

Security Assessment

DODO CrowdPooling V2

Dec 15th, 2021

Table of Contents

Summary

This report has been prepared for DODO CrowdPooling V2 to discover issues and vulnerabilities in the source code of the DODO CrowdPooling V2 project 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.

Additionally, this audit is based on a premise that all external smart contracts are safely implemented and all the mathematical formulas used in this project are correct.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing 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;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	DODO CrowdPooling V2
Platform	BSC, Ethereum, Polygon, Arbitrum, MoonRiver, Boba, Aurora
Language	Solidity
Codebase	https://github.com/DODOEX/contractV2/tree/starter/contracts/CrowdPooling
Commit	a0c7b5f72aa586f300f23e0344cdb3ed950d0659 d886097a1d9d4201f363cc9ecb08af34f966d484

Audit Summary

Delivery Date	Dec 15, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

Vulnerability Level	Total	ⓘ Pending	⊗ Declined	ⓘ Acknowledged	Partially Resolved	✓ Resolved
● Critical	0	0	0	0	0	0
● Major	1	0	0	1	0	0
● Medium	0	0	0	0	0	0
● Minor	0	0	0	0	0	0
● Informational	3	0	0	1	0	2
● Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
CPD	CP.sol	351b6131bceb531dc3cf6cf4a9d32e0df1cbe4e1fabfcad170c62606f4f40687
CPF	CPFunding.sol	fa82634b681a7c1c6886a8d590a4672a5cb69f4e0f754c4741b2b1a9f405ee0a
CPS	CPStorage.sol	18178485ac8ee2395861f6c7b4644e344b5ad7ccd72d3dd97b86f365ae5a2dcc
CPV	CPVesting.sol	3534acf53df0a82ecaa04cdf597e040cb3cfb633a0e3e82b58c3413496e2de70

Understandings

Overview

DODOCrowdPooling is the project that provides a new liquidity offering method that issues such as frontrunning, high cost of attracting liquidity, and/or insufficient liquidity. The workflow of the Crowpooling campaign is as below:

- The token issuer supplies a number of issued tokens and sets a soft cap target. A portion of the issued tokens will be used for crowdfunding and the rest will be used for ask-side liquidity in the pool. After the initial offering price, start and end time of the Crowdpooling campaign are set, anyone can participate in the offering by staking their capital.
- Once the Crowdpooling campaign ends, participates can claim the tokens based on their stakes at the pre-defined initial offering price. If the crowded capital is over the soft cap target, then all participate claim the surplus based on their shares of the pool.
- At the end of the Crowdpooling campaign, a new public liquidity pool will be automatically set up with the capital raised and the tokens reserved for ask-side liquidity.

At the same time, the DODOCrowdPooling project provides a pre-deposit settlement mechanism, liquidity protection mechanism, and support for flexible fee configuration.

- Pre-deposit settlement

  When the token issuer launches a Crowdpooling campaign, they need to pre-deposit the settlement fee into the contract. At the end of the Crowdpooling campaign, anyone can send a transaction to create the liquidity pool. The person will receive the pre-deposited settlement fee.

- Liquidity Protection

  The initial liquidity belongs to the creator of the Crowdpooling campaign, but the liquidity can not be removed during the liquidity protection period. Anyone is able to provide liquidity to these pools AMM-style, with the added benefit of higher capital efficiency thanks to PMM. This resulting spot market follows the bonding curve method, when a trader buys tokens, the token price goes up; when a trade sells tokens, the token price goes down.

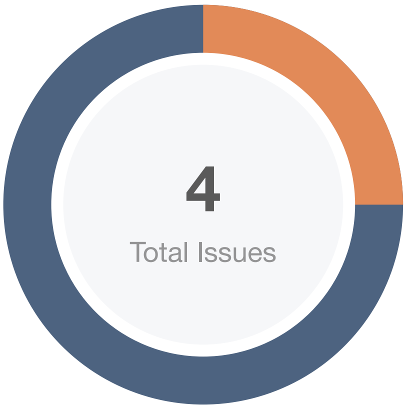
Privileged Functions

The contract contains the following privileged functions that are restricted by the `onlyOwner` modifier. They are used to modify the contract configurations and address attributes. We grouped these functions below:

The `onlyOwner` modifier:

- `claimLPToken()` in `CPVesting.sol`
- `forceStop()` in `CPStorage.sol`

Findings



🟥 **Critical**	**0** (0.00%)
🟧 **Major**	**1** (25.00%)
🟨 **Medium**	**0** (0.00%)
🟨 **Minor**	**0** (0.00%)
🟦 **Informational**	**3** (75.00%)
🟩 **Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Centralization Risk	**Centralization / Privilege**	● **Major**	ⓘ Acknowledged
CPD-01	Boolean Equality	Coding Style	● Informational	ⓘ Acknowledged
CPD-02	Missing Input Validation	Volatile Code, Inconsistency	● Informational	✓ Resolved
CPS-01	Unreasonable Modifier Name	Coding Style, Inconsistency	● Informational	✓ Resolved

GLOBAL-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Major	Global	ⓘ Acknowledged

Description

The role `owner` has the authority over the listed functions:

- `claimLPToken()` in `CPVesting.sol`
- `forceStop()` in `CPStorage.sol`

Any compromise to the key role account may allow a potential hacker to take advantage of this and execute malicious acts.

Recommendation

We advise the client to carefully manage the key role account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at the different levels in terms of short-term and long-term scenarios:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The client gave the following response:

`The new asset issuer, who uses the DODO platform, acts as the contract owner. The security of the owner depends on the security measures that taken by the new asset issuer, not DODO platform.`

CPD-01 | Boolean Equality

Category	Severity	Location	Status
Coding Style	● Informational	projects/DODO%20CrowdPooling%20V2/contracts/CP.sol (12a08a0): 27	ⓘ Acknowledged

Description

Detects the comparison to boolean constants. Boolean constants can be used directly and do not need to be compare to true or false.

Recommendation

We advise removing the equality to the boolean constant and referring to the following codes:

```
27  require(!_INITIALIZED_, "WE_NOT_SAVE_ETH_AFTER_INIT");
```

Alleviation

No alleviation.

CPD-02 | Missing Input Validation

Category	Severity	Location	Status
Volatile Code, Inconsistency	● Informational	projects/DODO%20CrowdPooling%20V2/contracts/CP.sol (12a08a0): 106~107	✓ Resolved

Description

The given input `switches` is missing the check for the length.

Recommendation

We advise adding the check for the passed-in values to prevent unexpected errors as below:

```
require(switches.length == 2, "CP: switches list length wrong");
```

Alleviation

The development team solved this issue at commit d886097a1d9d4201f363cc9ecb08af34f966d484.

CPS-01 | Unreasonable Modifier Name

Category	Severity	Location	Status
Coding Style, Inconsistency	● Informational	projects/DODO%20CrowdPooling%20V2/contracts/CPStorage.sol (12a08a0): 88	✓ Resolved

Description

According the usage logic of the linked modifier at L40, L74, and L115 in `CPFunding.sol`, the modified functions are allowed to execute if the vesting does not force to stop.

Recommendation

We advise that it's better to rename the modifier to `isNotForceStop()`.

Alleviation

The development team solved this issue at commit d886097a1d9d4201f363cc9ecb08af34f966d484.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK