Security Assessment

NEST-PVM

Jul 29th, 2022

Table of Contents

Summary

This report has been prepared for NEST-PVM to discover issues and vulnerabilities in the source code of the NEST-PVM 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.

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	NEST-PVM
Platform	Other
Language	Solidity
Codebase	https://github.com/NEST-Protocol/NEST-PVM-V1.0/commits/main/contracts
Commit	e521af6a332fa685b8e1ea5c639738943dceb10e

Audit Summary

Delivery Date	Jul 29, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

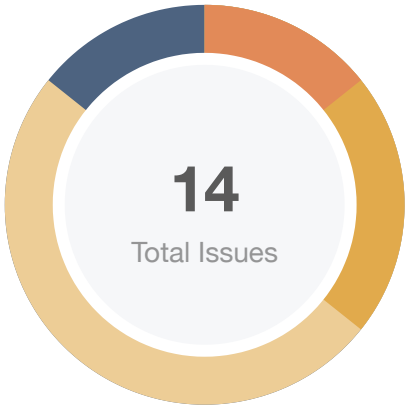
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
Critical	0	0	0	0	0	0	0
Major	2	0	0	2	0	0	0
Medium	3	0	0	3	0	0	0
Minor	7	0	0	7	0	0	0
Informational	2	0	0	2	0	0	0
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
NFN	NestFutures.sol	45114edafada31ae527abdc9c5eb4383867ec001cdb2354000d44c3aae0c365c
NON	NestOptions.sol	41b202adff90a6460f2a7725b056632026fc174612ea451018acb1dfdb3f073b
NBP	NestBuybackPool.sol	2a389ef7ac44cb880de70bf8900d65297392a139b3ffe43dd1e386da4d20905b
NVN	NestVault.sol	5707e54c5e3e80d5f7d1beec092f42de349ad42d99ce45df89bbe386c6b7a1d0

Findings



Critical	**0** (0.00%)
Major	**2** (14.29%)
Medium	**3** (21.43%)
Minor	**7** (50.00%)
Informational	**2** (14.29%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Financial Models	Logical Issue	Medium	Acknowledged
GLOBAL-02	Third Party Dependencies	Volatile Code	Minor	Acknowledged
NBP-01	Logic Issue On `DCU` Token	Logical Issue	Informational	Acknowledged
NES-01	Centralization Related Risks	**Centralization / Privilege**	**Major**	Acknowledged
NES-02	Lack Of Input Validation	Volatile Code	Minor	Acknowledged
NES-03	Incompatibility With Deflationary Tokens	Logical Issue	Minor	Acknowledged
NES-04	Mathematical Verification	Logical Issue	Minor	Acknowledged
NFN-01	Logical Issue Of Function `_balanceOf()`	Logical Issue	Minor	Acknowledged
NFN-02	Unreasonable Upper Boundary Of `lever`	Logical Issue	Informational	Acknowledged
NON-01	Calculation Of D1 Inconsistent With Whitepaper	Logical Issue	Major	Acknowledged
NON-02	Logical Issue About `ONE`	Logical Issue	Medium	Acknowledged
NON-03	Lack Of Validation Of `tokenIndex`	Logical Issue	Minor	Acknowledged
NON-04	Array Index Not Check	Volatile Code	Minor	Acknowledged

ID	Title	Category	Severity	Status
NVN-01	`allowance` Not Adjusted In Function `transferTo()`	Logical Issue	Medium	Acknowledged

GLOBAL-01 | Financial Models

Category	Severity	Location	Status
Logical Issue	Medium		Acknowledged

Description

There is no competition between investors and liquidity providers. The project pool contains all the funds, profits, and losses.

So the development team assumes the profit and loss are flat in the position part or they have sufficient liquidity or a robust operating strategy to maintain this pool in balance.

Financial models of blockchain protocols need to be resilient to attacks. They need to pass simulations and verifications to guarantee the security of the overall protocol. The financial model of this protocol is not in the scope of this audit.

Recommendation

We recommend the team elaborate on the pool operation strategy.

Alleviation

The team acknowledged this issue and they stated the following:

"The model is probabilistically favorable to the contract, and the system is a deflationary model: 1)minimum price limits for option buys, price drift coefficients for option calls and puts, and price scaling coefficients for option sells, which are set favorably to the contract 2) price drift coefficients for option buys and sells, and price correction coefficients, which are also favorable to the contract."

GLOBAL-02 | Third Party Dependencies

Category	Severity	Location	Status
Volatile Code	Minor		Acknowledged

Description

The contract is serving as the underlying entity to interact with third-party `INestBatchPrice2`, `INestGovernance`, and `Nest Token` protocols. The scope of the audit treats 3rd party entities as black boxes and assumes their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic requires interaction with `INestBatchPrice2`, `INestGovernance`, and `Nest Token`, etc. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

The team acknowledged this issue and they stated the following:

"The dependent contract is another module of NEST-Oracle, for which the latest version of the contract has been audited. And the operational status of the contract is always monitored."

NBP-01 | Logic Issue On `DCU` Token

Category	Severity	Location	Status
Logical Issue	Informational	NestBuybackPool.sol: 59, 66	Acknowledged

Description

In the contract `NestBuyBackPool`, `DCU` tokens are transferred to the current contract and swapped to `NEST` tokens, and the `Governance` account can call the function `migrate()` to transfer all `DCU` tokens from the contract to `NestLedger`. There is no guarantee that all `DCU` tokens will not be returned to the market.

Recommendation

We would like to confirm with the client if the current implementation aligns with the original project design.

Alleviation

The team acknowledged this issue and they stated the following:

"Repurchase is a system maintenance module, after the end of the repurchase, the repurchase contract NEST and DCU will be migrated to NestLedger contract, the DAO is responsible for maintenance, where NEST as a DAO assets at the disposal of the DAO, DCU by the DAO is responsible for unified destruction."

NES-01 | Centralization Related Risks

Category	Severity	Location	Status
Centralization / Privilege	**Major**	NestBuybackPool.sol: 49, 66; NestFutures.sol: 71, 188; NestOptions.sol: 71; NestVault.sol: 28, 39	Acknowledged

Description

In the contract `NestBuybackPool`, the account has governance permission over the following functions:

- function update(), to update the governance and the address of `DCU` token.
- function migrate(), to migrate funds from current contract to NestLedger.

Any compromise to the account with the governance permission may allow a hacker to take advantage of this authority.

In the contract `NestFutures`, the account has governance permission over the following functions:

- function register(), to register token configuration.
- function create(), to create future.

Any compromise to the account with the governance permission may allow a hacker to take advantage of this authority.

In the contract `NestVault`, the account has governance permission over the following functions:

- function update(), to update the governance and the address of `NEST` token.
- function approve(), to approve allowance amount to the target contract address.

Any compromise to the account with the governance permission may allow a hacker to take advantage of this authority.

In the contract `NestOptions`, the account has governance permission over the following functions:

- function register(), to register the token information.

Any compromise to the account with the governance permission may allow a hacker to take advantage of this authority.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

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

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement;
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles;
  OR
- Remove the risky functionality.

Noted: Recommend considering the long-term solution or the permanent solution. The project team shall make a decision based on the current state of their project, timeline, and project resources.

Alleviation

The team acknowledged the issue and they will adopt the multisign solution to ensure the private key management process in the future.

NES-02 | Lack Of Input Validation

Category	Severity	Location	Status
Volatile Code	Minor	NestFutures.sol: 71; NestOptions.sol: 71	Acknowledged

Description

The given input is missing the check for the token configuration.

Recommendation

We advise adding the check for the passed-in values to prevent unexpected error.

Alleviation

The team acknowledged this issue and stated they will make sure the settings are correct when they are maintained.

NES-03 | Incompatibility With Deflationary Tokens

Category	Severity	Location	Status
Logical Issue	Minor	NestBuybackPool.sol: 60; NestFutures.sol: 264; NestOptions.sol: 232	Acknowledged

Description

When transferring standard ERC20 deflationary tokens, the input amount may not be equal to the received amount due to the charged transaction fee.

Recommendation

We advise the client to regulate tokens supported and add necessary mitigation mechanisms to keep track of accurate balances if there is a need to support deflationary tokens.

Alleviation

The team acknowledged this issue and they stated `DCU` and `NEST` are not deflationary Tokens.

NES-04 | Mathematical Verification

Category	Severity	Location	Status
Logical Issue	Minor	NestFutures.sol: 408~413; NestOptions.sol: 245~252	Acknowledged

Description

The protocol is using some algorithms, including in the logic of the contract `NestFutures`, `NestOptions` etc. The Mathematical verification of these algorithms is not in the scope of this audit. The function logic will be checked based on the requirement documents.

Recommendation

We advise the client to revisit the design and ensure it is intended.

Alleviation

The team acknowledged this issue and stated they have tested the formula and so far the errors in the test results are within expectations.

NFN-01 | Logical Issue Of Function `_balanceOf()`

Category	Severity	Location	Status
Logical Issue	Minor	NestFutures.sol: 545~556	Acknowledged

Description

When the orientation is called,

$$balance: \ balance * (1 + lever * (\frac{oraclePrice}{basePrice} * \frac{2^{64}}{2^{64}+\mu*seconds} - 1))$$

the time factor and balance are inversely correlated, which means that the longer the account exists, the fewer the balance is.

While when the orientation is put,

$$balance: \ balance * (1 + lever * (1 - \frac{oraclePrice}{basePrice} * \frac{2^{64}}{2^{64}+\mu*seconds}))$$

they are positively correlated.

Recommendation

We would like to confirm with the client if the current implementation aligns with the original project design.

Alleviation

The team acknowledged this issue and they stated the following:

"After the user buys futures after determining the direction of the call and put and the leverage multiple, the actual amount of NEST it can obtain when selling is related to the current price and the price change of the reference price as a leverage multiple.

Since the prices of ETH and BTC have a certain trend in the long term, the reference price cannot be fixed at the same value as when it was bought and will change over time. In order to protect the contract, the system will set a relatively large growth rate for call futures and a relatively small growth rate for put futures. This is in line with expectations."

NFN-02 | Unreasonable Upper Boundary Of `lever`

Category	Severity	Location	Status
Logical Issue	Informational	NestFutures.sol: 403	Acknowledged

Description

The maximum lever of the future can be given as about 4294967296. We would like to confirm with the client if the current implementation aligns with the original project design.

Recommendation

We recommend adding a reasonable upper boundary to `lever`.

Alleviation

The team acknowledged this issue and they stated the following:

"There is no limit to the leverage limit in the design ,the limit in the contract is to prevent bit overflow when calculating the portfolio key."

NON-01 | Calculation Of D1 Inconsistent With Whitepaper

Category	Severity	Location	Status
Logical Issue	Major	NestOptions.sol: 617	Acknowledged

Description

According to the whitepaper, the formula is as below:

$$d_1 = \frac{1}{\sigma\sqrt{T}}[\ln\frac{S_0}{K} + (\mu + \frac{\sigma^2}{2})T],$$

$$d_2 = \frac{1}{\sigma\sqrt{T}}[\ln\frac{S_0}{K} + (\mu - \frac{\sigma^2}{2})T] = d_1 - \sigma\sqrt{T},$$

While in the contract, the formula is different:

$$d_1 = \frac{1}{\sigma\sqrt{T}}[\ln\frac{K}{S_0} + (\frac{\sigma^2}{2} - \mu)T] = -d_2.$$

Recommendation

We would like to confirm with the client if the current implementation aligns with the original project design.

Alleviation

The team acknowledged this issue and they stated the following:

"The new version of the white paper has transformed the option calculation formula and added the d2 expression, the formula used for the contract is before the transformation, the option calculation formula before and after the transformation is equivalent and has been verified."

NON-02 | Logical Issue About `ONE`

Category	Severity	Location	Status
Logical Issue	Medium	NestOptions.sol	Acknowledged

Description

In the contract, the value of the variable `ONE` is 2^{64}. And it's used in many algorithms.

For example, $d1 = \frac{1}{\sigma\sqrt{T}}[\ln\frac{K}{S0} + 64\ln 2 + (-\mu + \frac{\sigma^2}{2})T]$.

And at line 580, $left = (\mu T + one)(one - \_snd(d - \sigma\sqrt{T}))$,

since $one^2 \neq one$, the factor should be paid attention to in the calculation. The project team should fully test its functionality to guarantee its feasibility.

Recommendation

We recommend the team check the logic and fix the issue.

Alleviation

The team acknowledged this issue and they stated the following:

"The contract code is a multiplication calculation using the ABDKMath64x64 library, which represents the number as a 64-bit binary decimal, and automatically performs the decimal part of the calculation, which results in ONE when calculating ABDKMath64x64.mul(ONE, ONE)."

NON-03 | Lack Of Validation Of `tokenIndex`

Category	Severity	Location	Status
Logical Issue	Minor	NestOptions.sol: 203	Acknowledged

Description

The function `open()` lacks validation on the variable `tokenIndex`. To ensure the token is supported and its config is valid, it's recommended to add validation on the `tokenIndex`.

Recommendation

We recommend the team check the logic and fix the issue.

Alleviation

The team acknowledged this issue and they will leave it as it is for now.

NON-04 | Array Index Not Check

Category	Severity	Location	Status
Volatile Code	Minor	NestOptions.sol: 266, 315	Acknowledged

Description

The input parameter `index` is not checked for a valid array index.

Recommendation

We recommend adding the sanity check to ensure the index stays within the array range.

Alleviation

The team acknowledged this issue and they will leave it as it is for now.

NVN-01 | `allowance` Not Adjusted In Function `transferTo()`

Category	Severity	Location	Status
Logical Issue	Medium	NestVault.sol: 46	Acknowledged

Description

In the `transferTo()`, there is no adjustment of the msg.sender's `allowance`. This results in an address always being able to transfer the allowed amount.

Recommendation

We recommend adjusting the `allowance` after calling the function `transferTo()`.

Alleviation

The team acknowledged this issue and they stated the following:

"NestVault is used as a system pool to authorize options and futures contracts to use the funds in the pool to settle with users. The allowance is limited to a fixed value to prevent system errors from distributing too many NESTs to users, so it is a maximum amount, not an authorized amount."

Optimizations

ID	Title	Category	Severity	Status
NVN-02	Missing Emit Events	Coding Style	Optimization	Resolved

NVN-02 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Optimization	NestVault.sol: 39	Resolved

Description

The function that affects the status of sensitive variables should be able to emit events as notifications.

Recommendation

Consider adding events for sensitive actions, and emit them in the function.

Alleviation

The team heeded our advice and resolved this issue in commit `560b5e337d302724df4e4b9529685c50c6a17194`.

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.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

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.

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.