Code Security Assessment

Goldefy

Mar 2nd, 2022

Table of Contents

Summary

This report has been prepared for Goldefy to discover issues and vulnerabilities in the source code of the Goldefy 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	Goldefy
Description	ERC20
Platform	BSC
Language	Solidity
Codebase	Files provided by the client
Commit	

Audit Summary

Delivery Date	Mar 02, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

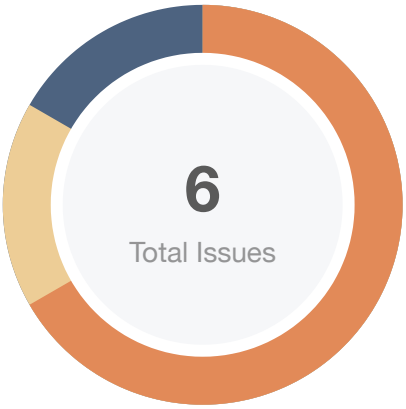
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Mitigated	Resolved
Critical	0	0	0	0	0	0	0
Major	4	0	0	4	0	0	0
Medium	0	0	0	0	0	0	0
Minor	1	0	0	0	1	0	0
Informational	1	0	0	1	0	0	0
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
ERM	token/ERC20/behaviours/ERC20Mintable.sol	a6df26859ab36ecbd5e71eb7b354b7429b121919cfb856fe1579a109fa334464
GER	token/ERC20/GoldefyERC20.sol	99b87b91f42aff5a6dc59c41246e52cbd6f0a261ac4e8922254d6c93c7cf539e

Findings



Critical	**0** (0.00%)
Major	**4** (66.67%)
Medium	**0** (0.00%)
Minor	**1** (16.67%)
Informational	**1** (16.67%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
GER-01	Initial Token Distribution	**Centralization / Privilege**	**Major**	Acknowledged
GER-02	Mintable Token	**Centralization / Privilege**	**Major**	Acknowledged
GER-03	Invisible Implementation of Contract `antisnipe`	Volatile Code	Major	Acknowledged
GER-04	Third Party Dependencies	Volatile Code	Minor	Partially Resolved
GER-05	Centralization Risk in GoldefyERC20.sol	**Centralization / Privilege**	**Major**	Acknowledged
GER-06	Missing Error Messages	Coding Style	Informational	Acknowledged

GER-01 | Initial Token Distribution

Category	Severity	Location	Status
Centralization / Privilege	Major	token/ERC20/GoldefyERC20.sol: 48	Acknowledged

Description

```
39      constructor (
40          string memory name,
41          string memory symbol,
42          uint8 decimals,
43          uint256 initialBalance
44      )
45          ERC1363(name, symbol)
46      {
47          _setupDecimals(decimals);
48          _mint(_msgSender(), initialBalance);
49      }
```

`initialBalance` Goldefy tokens are sent to the contract deployer when deploying the contract. This could be a centralization risk as the deployer can distribute Goldefy tokens without obtaining the consensus of the community.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key.

Alleviation

The team has acknowledged this finding.

GER-02 | Mintable Token

Category	Severity	Location	Status
Centralization / Privilege	Major	token/ERC20/GoldefyERC20.sol: 70~72	Acknowledged

Description

Function `mint()` in contract `ERC20Mintable`:

```
44      function mint(address account, uint256 amount) public canMint {
45          _mint(account, amount);
46      }
```

Function `_mint()` in contract `GoldefyERC20`:

```
70      function _mint(address account, uint256 amount) internal override onlyMinter {
71          super._mint(account, amount);
72      }
```

Modifier `onlyMinter()` in contract `Roles`:

```
20      modifier onlyMinter() {
21          require(hasRole(MINTER_ROLE, _msgSender()), "Roles: caller does not have the MINTER
role");
22          _;
23      }
```

The role `MINTER_ROLE` in contract `GoldefyERC20` has authority over the function `_mint()`. Any compromise to the account may allow a hacker to take advantage of this authority and mint tokens to any account.

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

[Goldefy Team]:

1. Mint related functions will be managed through Openzeppelin Defender and Gnosis Safe, and multisig based on 3 of 4 minting will be applied.
2. The Gnosis Safe address is designated as the Contract Default Admin Role in the contract creator.
3. The account address to participate in Multi-Sig will be announced on the homepage, Medium and blog.

GER-03 | Invisible Implementation Of Contract `antisnipe`

Category	Severity	Location	Status
Volatile Code	Major	token/ERC20/GoldefyERC20.sol: 51	Acknowledged

Description

```
51    IAntisnipe public antisnipe = IAntisnipe(0xbccE75E1b2C953C83B462F80865f408112CE29A2);
```

```
86    function _beforeTokenTransfer(
87      address from,
88      address to,
89      uint256 amount
90    ) internal override {
91      if (from == address(0) || to == address(0)) return;
92      if (liquidityRestrictionEnabled && address(liquidityRestrictor) != address(0)) {
93          (bool allow, string memory message) = liquidityRestrictor
94              .assureLiquidityRestrictions(from, to);
95          require(allow, message);
96      }
97
98      if (antisnipeEnabled && address(antisnipe) != address(0)) {
99          require(antisnipe.assureCanTransfer(msg.sender, from, to, amount));
100     }
101   }
```

The implementation of contract `antisnipe` is invisible on BscScan, so we are unable to evaluate its functionality and security.

Recommendation

We recommend verifying and publishing the code of contract `antisnipe` on BscScan.

Alleviation

The team has acknowledged this finding.

GER-04 | Third Party Dependencies

Category	Severity	Location	Status
Volatile Code	Minor	token/ERC20/GoldefyERC20.sol: 51~52	Partially Resolved

Description

The contract `GoldefyERC20` is serving as the underlying entity to interact with third parties `antisnipe` and `liquidityRestrictor` 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.

Moreover, the addresses of these third parties can be updated through functions `setAntisnipeAddress()` and `setLiquidityRestrictionAddress()`.

Recommendation

We understand that the business logic of `GoldefyERC20` requires interaction with `antisnipe` and `liquidityRestrictor`. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[Goldefy Team]: It is a contract that is already being used in other NFT and DeFi related projects, and if an error occurs in the contract, the method for immediate stop and address change is implemented as a fallback as follows:

- setAntisnipeDisable
- setLiquidityRestrictorDisable
- setAntisnipeAddress
- setLiquidityRestrictionAddress

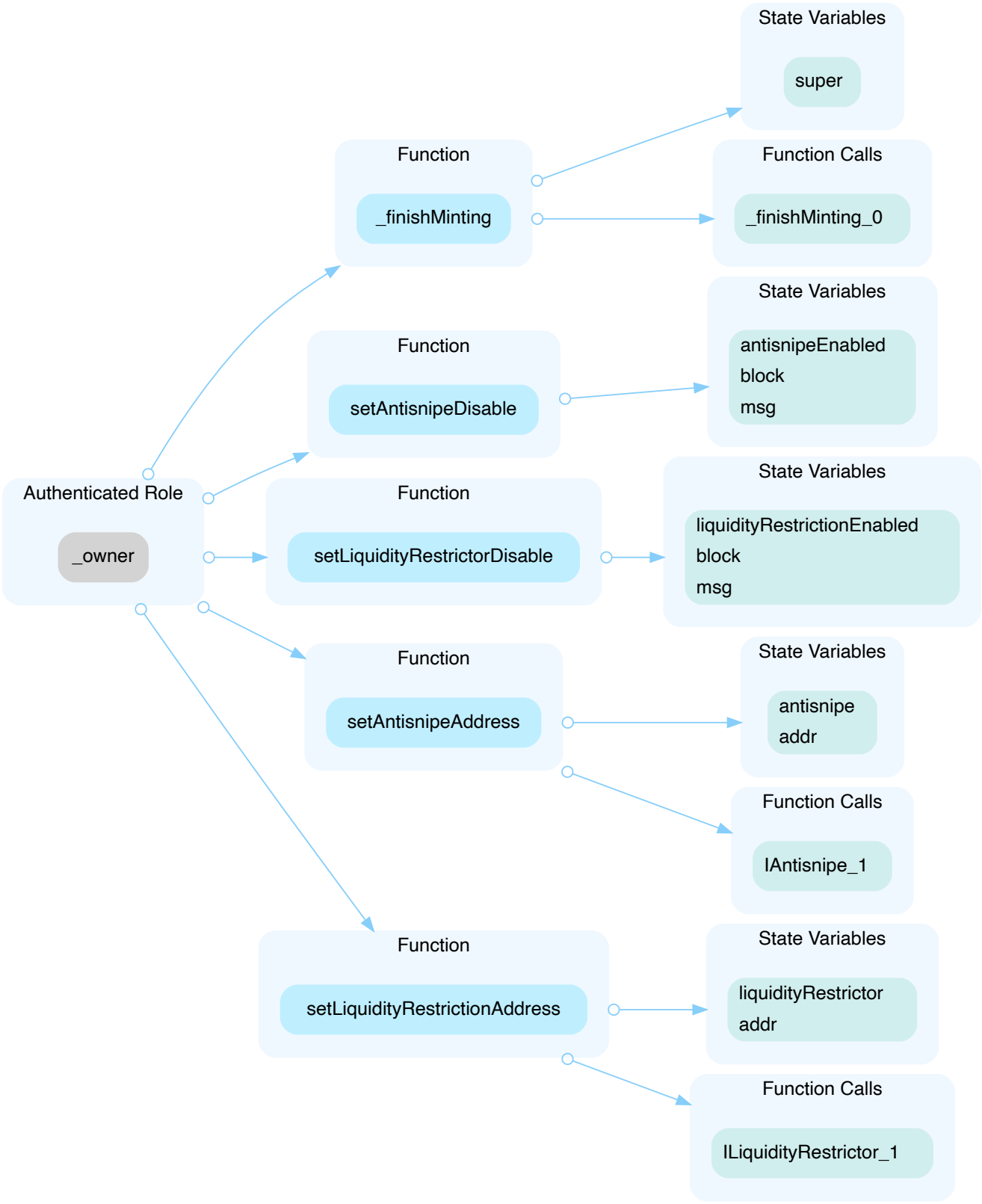
GER-05 | Centralization Risk In GoldefyERC20.sol

Category	Severity	Location	Status
Centralization / Privilege	**Major**	token/ERC20/GoldefyERC20.sol: 79~81, 106~110, 115~119, 124~127, 132~135	Acknowledged

Description

In the contract, `GoldefyERC20`, the role, `_owner`, has authority over the functions shown in the diagram below.

Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and related functions.



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., multisignature 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.

Alleviation

[Goldefy Team]:

1. We plan to manage related functions through Openzeppelin Defender and Gnosis Safe, and apply multisig of 3 of 4 standards.
2. Processed to designate the Gnosis Safe address as the Contract Default Admin Role to the contract creator.
3. The account address to participate in Multi-Sig will be announced on the homepage, Medium and blog

GER-06 | Missing Error Messages

Category	Severity	Location	Status
Coding Style	Informational	token/ERC20/GoldefyERC20.sol: 99, 107, 116	Acknowledged

Description

The **require** can be used to check for conditions and throw an exception if the condition is not met. It is better to provide a string message containing details about the error that will be passed back to the caller.

Recommendation

We advise adding error messages to the linked **require** statements.

Alleviation

The team has acknowledged this finding.

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.

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.