



Security Assessment

Joltify.io / Joltify.finance

Nov 28th, 2021

Table of Contents

Summary

Overview

[Project Summary](#)

[Audit Summary](#)

[Vulnerability Summary](#)

[Audit Scope](#)

Findings

[JCC-01 : Centralization Risk](#)

[SCK-01 : Incompatibility With Deflationary Tokens](#)

[SCK-02 : Parameters possible to change during Staking](#)

[SCK-03 : `descMonthly` not used](#)

[SCK-04 : Centralization Risk](#)

[SCK-05 : Missing emit events](#)

[SCK-06 : Division Before Multiplication](#)

Appendix

Disclaimer

About

Summary

This report has been prepared for Joltify.io to discover issues and vulnerabilities in the source code of the Joltify.io / Joltify.finance 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	Joltify.io / Joltify.finance
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/joltify-finance/token-staking.git https://github.com/joltify-finance/joltify-token.git
Commit	9ef5f46355c7e04ba4cd491e16941e14b036c281 409a408d5b671482f5e90a202175922334dae413 2f7b150e35e6d31813364779c043ac0c425e2102

Audit Summary

Delivery Date	Nov 28, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

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

Audit Scope

ID	File	SHA256 Checksum
JCC	projects/projects/joltify/contracts/JoltifyCoin.sol	d224513e8fb84afaaaf37aef7e0b82c9797ae31ee31ced2ac3b8511b44855547
SCK	projects/projects/joltify/contracts/Staking.sol	72a933242cfd9f60a080c10e5579f152566bcb135b3bec1505d20bff218c3681

Findings



Critical	0 (0.00%)
Major	2 (28.57%)
Medium	0 (0.00%)
Minor	3 (42.86%)
Informational	2 (28.57%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
JCC-01	Centralization Risk	Centralization / Privilege	● Major	⌚ Partially Resolved
SCK-01	Incompatibility With Deflationary Tokens	Volatile Code	● Informational	ⓘ Acknowledged
SCK-02	Parameters possible to change during Staking	Logical Issue	● Minor	✓ Resolved
SCK-03	<code>descMonthly</code> not used	Gas Optimization	● Minor	✓ Resolved
SCK-04	Centralization Risk	Centralization / Privilege	● Major	⌚ Partially Resolved
SCK-05	Missing emit events	Coding Style	● Informational	✓ Resolved
SCK-06	Division Before Multiplication	Mathematical Operations	● Minor	✓ Resolved

JCC-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Major	projects/projects/joltify/contracts/JoltifyCoin.sol	🕒 Partially Resolved

Description

In the contract `JoltifyCoin`, the role `MINTER_ROLE` has the authority over the following function:

- mint

Any compromise to the `MINTER_ROLE` account may allow the hacker to take advantage of this and mint token to an arbitrary address.

the role `PAUSER_ROLE` has the authority over the following function:

- unpause
- pause

Any compromise to the `PAUSER_ROLE` account may allow the hacker to take advantage of this and mint token to an arbitrary address.

The deployer of the contract has the ability to set/revoke roles, and the deployer is `MINTER_ROLE` and `PAUSER_ROLE` when the contract deployed.

Recommendation

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 to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

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

- 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

[Joltify Team]: We assign the privileged role “MINTER_ROLE/Admin_ROLE/PAUSE_ROLE” , to multi-signature wallet contract to prevent a single point of failure due to the private key. We take advantage of Gnosis-safe to deploy the multi-signature wallet on the Binance smart chain. The multi-signature wallet address is

<https://gnosis-safe.io/app/bnb:0x2B0417D30a5f00b67E1aBCFBE38F194d9c85AD48/settings/policies>

SCK-01 | Incompatibility With Deflationary Tokens

Category	Severity	Location	Status
Volatile Code	● Informational	projects/projects/joltify/contracts/Staking.sol	ⓘ 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. For example, if a user stakes 100 deflationary tokens (with a 10% transaction fee) in a MasterChef, only 90 tokens actually arrived in the contract. However, the user can still withdraw 100 tokens from the contract, which causes the contract to lose 10 tokens in such a transaction.

Reference: <https://thoreum-finance.medium.com/what-exploit-happened-today-for-gocerberus-and-garuda-also-for-lokum-ybear-piggy-caramelswap-3943ee23a39f>

Recommendation

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

Alleviation

[Joltify Team]:

We confirm that JOLT, the staking token we use is not deflationary

SCK-02 | Parameters possible to change during Staking

Category	Severity	Location	Status
Logical Issue	● Minor	projects/projects/joltify/contracts/Staking.sol	🕒 Resolved

Description

Multiple parameters that are related to staking reward calculation is interchangeable after the staking starts, which might mess up the reward calculation for certain users.

Recommendation

We recommend the client to confirm that this is the intended behavior.

Alleviation

[Joltify Finance Team]: we have updated the code logic of the APR and the calculate the APR for users separately once we have adjust the APRs.

SCK-03 | descMonthly not used

Category	Severity	Location	Status
Gas Optimization	● Minor	projects/projects/joltify/contracts/Staking.sol: 40	✓ Resolved

Description

descMonthly is not used in the contract.

Recommendation

we recommend removing unused components from the contract.

Alleviation

[Joltify Team]: The variable descMonthly have been removed.

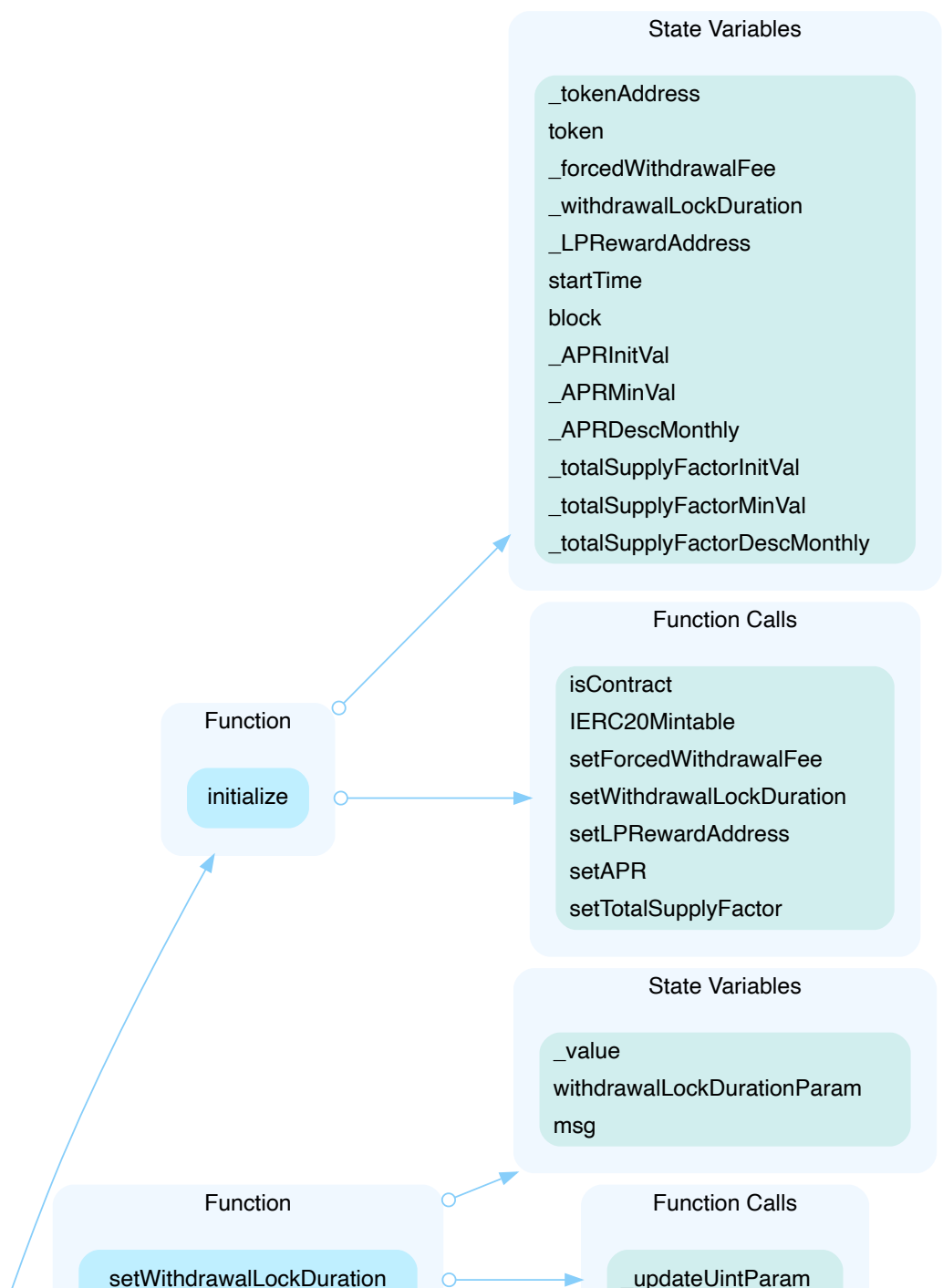
SCK-04 | Centralization Risk

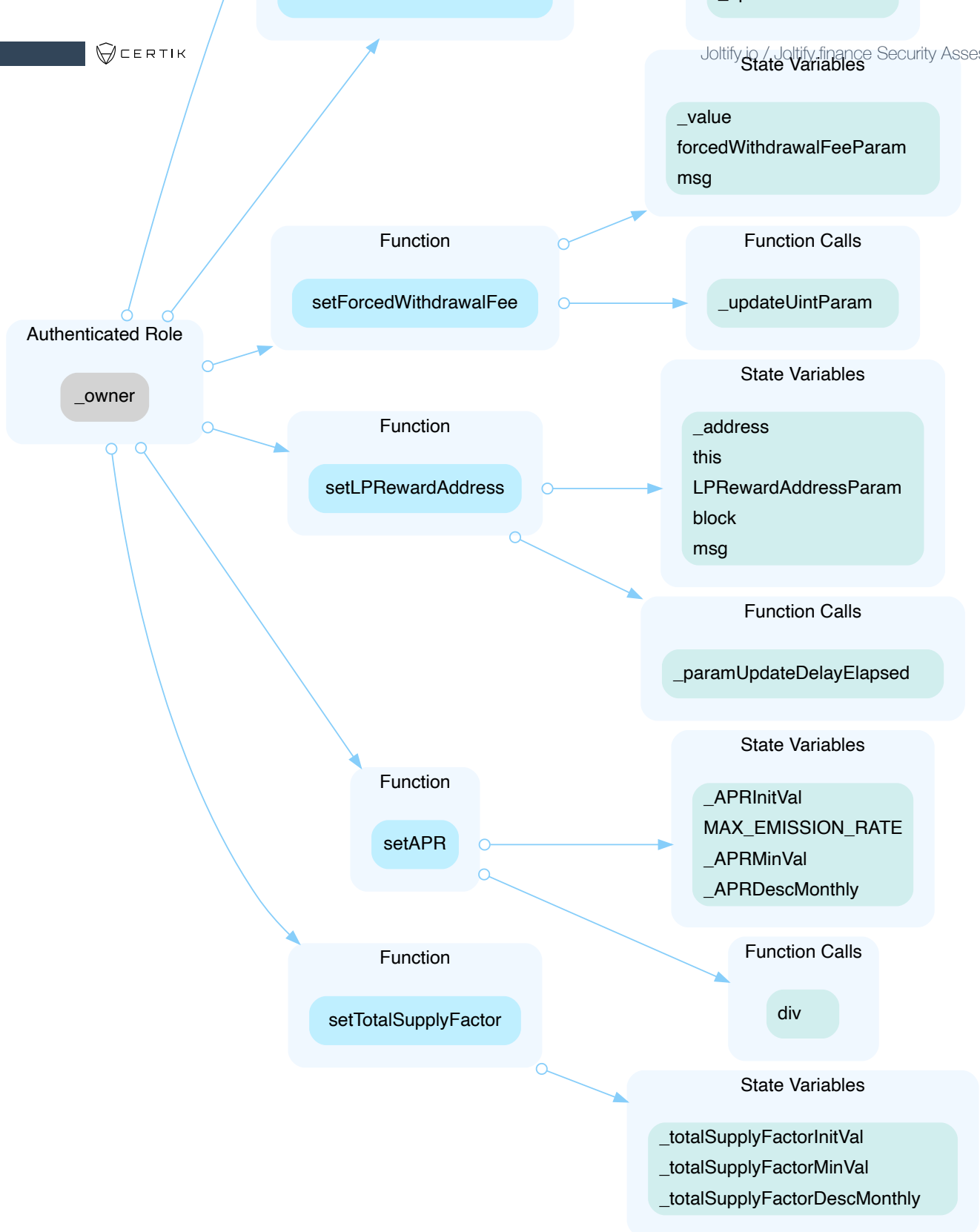
Category	Severity	Location	Status
Centralization / Privilege	● Major	projects/projects/joltify/contracts/Staking.sol: 59~79, 91~95, 102~106, 113~126, 151~156, 158~163	🔄 Partially Resolved

Description

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

Any compromise to the privileged account which has access to `_owner` may allow the hacker to take advantage of this.





Recommendation

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 to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g.,

Multisignature wallets.

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

- 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

[Joltify Team]: We assign the privileged role “MINTER_ROLE/Admin_ROLE/PAUSE_ROLE” , to multi-signature wallet contract to prevent a single point of failure due to the private key. We take advantage of Gnosis-safe to deploy the multi-signature wallet on the Binance smart chain. The multi-signature wallet address is

<https://gnosis-safe.io/app/bnb:0x2B0417D30a5f00b67E1aBCFBE38F194d9c85AD48/settings/policies>

SCK-05 | Missing emit events

Category	Severity	Location	Status
Coding Style	● Informational	projects/projects/joltify/contracts/Staking.sol: 59~79, 151~156, 158~163	👍 Resolved

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Alleviation

[Joltify Team]: We have added all events for functions which need event.

SCK-06 | Division Before Multiplication

Category	Severity	Location	Status
Mathematical Operations	● Minor	projects/projects/joltify/contracts/Staking.sol: 82~86	✓ Resolved

Description

Mathematical operations in the linked function perform divisions before multiplications. Performing multiplication before division can sometimes avoid loss of precision.

Recommendation

We advise the client to apply multiplications before divisions if integer overflow would not happen in functions.

Alleviation

[Joltify Team]: All divisions have been moved to the end.

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.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Mathematical Operations

Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.

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.

