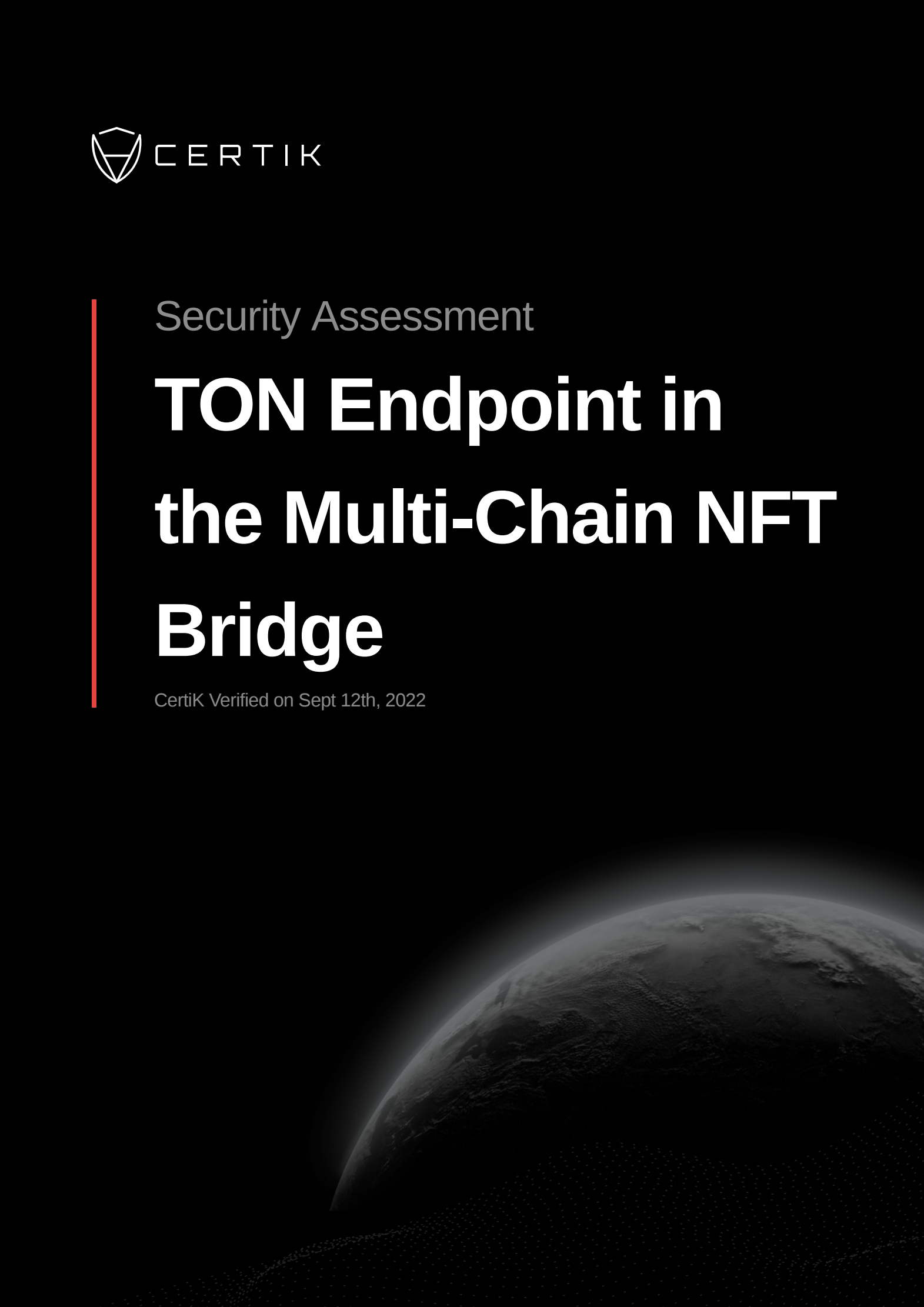
CERTIK

Security Assessment

TON Endpoint in the Multi-Chain NFT Bridge

CertiK Verified on Sept 12th, 2022



CertiK Verified on Sept 12th, 2022

TON Endpoint in the Multi-Chain NFT Bridge

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Bridge	TON	Manual Review

LANGUAGE	TIMELINE	KEY COMPONENTS
FunC	Delivered on 09/12/2022	N/A

CODEBASE

https://github.com/XP-NETWORK/xp-the-open-network

View All

COMMITS

base cf06590e792aeb62f977b841ebc33bf9a08e7fed

update1 a628f13a5320e700456f0f052d597a8f0e7761ed...

View All

Vulnerability Summary

9	8	1	0	0	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
1	Major	1 Mitigated	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
2	Medium	2 Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
3	Minor	3 Resolved	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
3	Informational	3 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

CODEBASE | TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

Repository

https://github.com/XP-NETWORK/xp-the-open-network

Commit

base cf06590e792aeb62f977b841ebc33bf9a08e7fed
update1 a628f13a5320e700456f0f052d597a8f0e7761ed
update2 c177605c0401b492c62b1080f644bc3ef11e1111

AUDIT SCOPE | TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

9 files audited ● 1 file with Mitigated findings ● 1 file with Resolved findings ● 7 files without findings

ID	File	SHA256 Checksum
XPN	bridge.func	27f0336300acc378b03f357083ec990a23a59464b1225b4b08059225089aa2c1
XPE	burner.func	e9ad29e833a4c8d06a5a9447e8956d50b38b2e347af37cce706659520c745179
XPT	op-codes.fc	e25604a74fed44d484af0b68267f9f270dcd075a9b1d34441ed9817d714e0135
XPR	bridge.func	172fa160c641c34871e454b4d21dbc008812ae863d9288db719ea21fd19c5ffc
XPK	burner.func	a5458c008f2c8e5587e7facff1e7a2303d365979033eea3d9e0c245eee06f627
XNE	op-codes.fc	e25604a74fed44d484af0b68267f9f270dcd075a9b1d34441ed9817d714e0135
XNK	bridge.func	4475ed632d058eb4ce1859a42f8e000b2ef19593865d9b7669b4177ca08360d0
XET	burner.func	a5458c008f2c8e5587e7facff1e7a2303d365979033eea3d9e0c245eee06f627
XEW	op-codes.fc	e25604a74fed44d484af0b68267f9f270dcd075a9b1d34441ed9817d714e0135

APPROACH & METHODS

TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

This report has been prepared for XP.Network to discover issues and vulnerabilities in the source code of the TON Endpoint in the Multi-Chain NFT Bridge project. A comprehensive examination has been performed, utilizing Manual Review technique.

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 maintainability perspective:

- Perform the audit of other parts of the bridge. It is unclear what events are monitored by the off-chain part.
- Provide more transparency on general communication workflow in code comments.

FINDINGS | TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

9	0	1	2	3	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for TON Endpoint in the Multi-Chain NFT Bridge. Through this audit, we have uncovered 9 issues ranging from different severity levels. Utilizing Static Analysis techniques to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
XPN-01	**Centralization Related Risks**	**Centralization / Privilege**	**Major**	**Mitigated**
XPE-01	"Replay Failed" Attack Can Drain All The Balance	Language Specific	Medium	Resolved
XPN-02	`this_address` Is Not Checked In "Change Public Key" Method	Logical Issue	Medium	Resolved
XPN-03	The Meaning Of `action_id` Is Unclear	Inconsistency	Minor	Resolved
XPN-04	Pull-Over-Push Pattern	Logical Issue	Minor	Resolved
XPN-05	`end_parse()` Is Missing	Coding Style	Minor	Resolved
XPE-02	Redundant Statements	Coding Style	Informational	Resolved
XPN-06	`recv_internal()` Should Be Refactored	Coding Style	Informational	Resolved
XPN-07	No Ability To Remove From "Whitelist"	Logical Issue	Informational	Resolved

XPN-01 | FINDING DETAILS

Finding Title

Centralization Related Risks

Category	Severity	Location	Status
Centralization / Privilege	**Major**	**bridge.func (base): 40~41**	**Mitigated**

Description

The owner of `public_key` has authority to:

- mint new tokens in the owned `nft_collection`
- transfer minted/frozen tokens to any address
- withdraw fees
- change public key
- whitelist `nft_collection` s
- pause/unpause the bridge

A compromise of this account allows the hacker to withdraw all the tokens frozen and completely block the bridge work.

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.

For example, "3 of 3" multi-signature wallet can be assigned as the bridge owner. And 3 independent bridge operators can control that wallet. That will significantly increase the bridge security.

Alleviation

[**XP.Network**]: At the moment, the oracles reside on seven physically different machines. Geographically they are in Israel & Europe. The threshold is 5/7 signatures. The oracles are controlled by three organizations, one of which is XP.Network. FROST threshold Schnorr signature protocol is used with secret shared over oracles.

XPE-01 | FINDING DETAILS

Finding Title

"Replay Failed" Attack Can Drain All The Balance

Category	Severity	Location	Status
Language Specific	Medium	burner.func (base): 18~28	Resolved

Description

Burner `recv_external()` works this way:

- Signature checked
- Message accepted
- Raw messages sent
- `stored_seqno` incremented

According to documentation, if after `accept_message()` some error will be thrown (both in ComputePhase or ActionPhase) transaction will be written to blockchain and fees will be deducted from contract balance, but storage will not be updated and actions will not be applied as in any transaction with error exit code. That way, if contract accepted external message and then throw an exception due to some error in message data or due to sending wrongly serialized message, it will pay for processing but has no opportunity to prevent message replay. The same message will be accepted by contract over and over until it consumes the whole balance.

Recommendation

We recommend rewriting the function this way:

```
17   throw_unless(35, check_signature(slice_hash(in_msg), signature, public_key));
18   accept_message();
19
20   set_data(begin_cell()
21     .store_uint(stored_seqno + 1, 32)
22     .store_uint(stored_subwallet, 32)
23     .store_uint(public_key, 256)
24     .end_cell());
25   commit();
26
27   cs~touch();
28   while (cs.slice_refs()) {
29     var mode = cs~load_uint(8);
30     send_raw_message(cs~load_ref(), mode);
31   }
```

XPN-02 | FINDING DETAILS

Finding Title

`this_address` Is Not Checked In "Change Public Key" Method

Category	Severity	Location	Status
Logical Issue	Medium	bridge.func (base): 218~219	Resolved

Description

`this_address` is loaded from incoming message, however, not compared to `my_address()`. This opens a "replay attack" vector - the signed message from the testnet or another deployment of the contract can be reused on mainnet.

Recommendation

We recommend checking that `equal_slices(this_address, my_address())`.

XPN-03 | FINDING DETAILS

Finding Title

The Meaning Of `action_id` Is Unclear

Category	Severity	Location	Status
Inconsistency	Minor	bridge.func (base): 142~158, 343~347	Resolved

Description

The contract contains `action_id` field, it can be retrieved via `get_action_id()` get-method. The value is incremented as a reaction on `op::ownership_assigned()` and `op::excesses()`. In addition the contract accepts `action_id` as part of incoming message, it is saved in `consumed_actions`.

This leads to a confusion. The meaning of the first field is unclear. It can be influenced by any third-party. The code of `op::ownership_assigned()` and `op::excesses()` processing is redundant and can be omitted.

Recommendation

We recommend removing the contract field or clarifying the intended logic via code comments.

Alleviation

XP.Network opted not to change the name of the `action_id` field and get-method and not to add additional code comments. The field is used by off-chain oracles to monitor if tokens were transferred to the bridge contract. The oracle will not "vote" for the same `action_id` for the second time.

XPN-04 | FINDING DETAILS

Finding Title

Pull-Over-Push Pattern

Category	Severity	Location	Status
Logical Issue	Minor	bridge.func (base): 219~220	Resolved

Description

The change of `public_key` by function "change public key" is done without guaranteeing the `new_public_key` is able to actuate transactions on-chain. For example, zero value can be assigned by mistake.

Recommendation

We advise the pull-over-push pattern to be applied here whereby a `new_public_key` is first proposed and consequently needs to be accepted ensuring that the account can actuate transactions on-chain.

XPN-05 | FINDING DETAILS

Finding Title

`end_parse()` Is Missing

Category	Severity	Location	Status
Coding Style	Minor	bridge.func (base): 7~8, 51~52, 101~102, 165~166, 212~213, 240~241, 273~274, 302~303	Resolved

Description

`end_parse()` checks if slice is empty, otherwise throws an exception. It allows to ensure the slice has the expected data structure.

Recommendation

We recommend using `end_parse()` wherever possible.

XPE-02 | FINDING DETAILS

Finding Title

Redundant Statements

Category	Severity	Location	Status
Coding Style	Informational	burner.func (base): 45~69	Resolved

Description

The linked statements do not affect the functionality of the codebase and appear to be leftovers from test code.

Recommendation

We recommend removing of unused code.

XPN-06 | FINDING DETAILS

Finding Title

`recv_internal()` Should Be Refactored

Category	Severity	Location	Status
Coding Style	Informational	bridge.func (base): 29~30	Resolved

Description

`recv_internal()` function contains 300 lines and implements different functionality. A lot of code is duplicated many times.

Recommendation

We recommend refactoring the function and creating separate functions for each logical block.

XPN-07 | FINDING DETAILS

Finding Title

No Ability To Remove From "Whitelist"

Category	Severity	Location	Status
Logical Issue	Informational	bridge.func (base): 234~235	Resolved

Description

There is no ability to remove items from the whitelist. In case some `nft_collection` is compromised, it will never be deleted from the whitelist.

Recommendation

We recommend adding the functionality to delete items from the whitelist.

APPENDIX | TON ENDPOINT IN THE MULTI-CHAIN NFT BRIDGE

Finding Categories

Categories	Description
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.
Language Specific	Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.
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 | CERTIK

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.

CertiK | Securing the Web3 World

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.