Code Security Assessment

Kyberdyne

Feb 18th, 2022

Table of Contents

Summary

This report has been prepared for Kyberdyne to discover issues and vulnerabilities in the source code of the Kyberdyne 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	Kyberdyne
Platform	Other
Language	Solidity
Codebase	https://github.com/kyberdyne-game/game-contracts/tree/audit/contracts
Commit	87fff7ac23e6cbe2243d1f861755161ff6f8025d

Audit Summary

Delivery Date	Feb 18, 2022
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	3	0	0	3	0	0	0
Medium	1	0	0	1	0	0	0
Minor	2	0	0	0	0	0	2
Informational	1	0	0	1	0	0	0
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
HER	depends/erc20improved/HERC20IMEvent.sol	9d4d525c339cabc239d3d8118d7fb8327c8b9b86b87a9be1b692c020a97fa7f3
HEC	depends/erc20improved/HERC20IMInterface.sol	6923626821992892bd0b51125573ce2881eea285d54d18f3a55f70096e827c74
HEI	depends/erc20improved/HERC20IMLayout.sol	b54e7045a2cc9e2610f17ee658b1a683fb11cfcb08dad6605ac7b8b2ed2df687
HEM	depends/erc20improved/HERC20IMLogic.sol	646dec8b2ab6257975127959be7f0077d5d27e033f0fc758a57a328951c15f13
HEL	depends/erc20improved/HERC20IMLogicBase.sol	3aab9fb2ebcf9d0f1be2b4ffeaa5a15df571ac46dcd200b5544a9b0be4e71ce1
HES	depends/erc20improved/HERC20IMStorage.sol	5e6e3aa86f032ce52094d2a19815efc01190147f27fda9dc6022a63f7d382f23
HET	depends/erc20improved/HERC20IMType.sol	116cd66ed83c6b0e8de868dd57232b832a37acb792aedf5f49a99062099ccc12
HEE	depends/erc721improved/HERC721IMEvent.sol	23064abdb1b24b55954bdc5885ce0a219580a250da15a2efe41fa7ea10e0970c
HRC	depends/erc721improved/HERC721IMInterface.sol	0cef499fbfa29b3f4156385cc9b492af3075d7c9e385cb16a6fed982409b5aed
HRI	depends/erc721improved/HERC721IMLayout.sol	f5168dff811254f765deae4012270b7186b45fd6d99d1d81d8a5cadbe35e4355
HRM	depends/erc721improved/HERC721IMLogic.sol	87791dd7b25043debbd98612effd707371a52458ea3ba327bf77e43e4d1c73b2
HEB	depends/erc721improved/HERC721IMLogicBase.sol	d47c4339ac4252b3a6ecde12d365aa0f1ef3908406ec025d929337abb42eda36
HRS	depends/erc721improved/HERC721IMStorage.sol	3bfa1fe5df8b920f8f8c4a6475256abc6940de95895bd49f7736b3b91fa905ec
HRT	depends/erc721improved/HERC721IMType.sol	63d8576232637ac6b78750f4fb4d2b10327a0b880a03bff1a6f6a9a4e9ada2a2

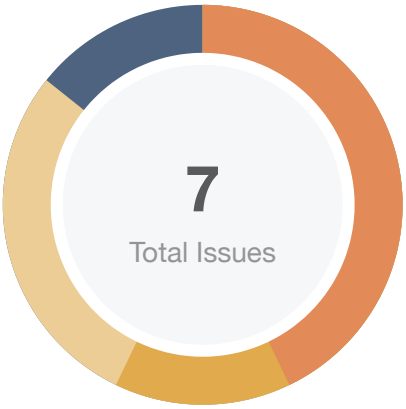
ID	File	SHA256 Checksum
KBD	kbdNameService/KBDNameServiceEvent.sol	73efa71bb40c6264af50fb3f4e4660e22379940ce287057e5ee5fea88b8f9b9f
KBN	kbdNameService/KBDNameServiceInterface.sol	e11059bae0c80f880629dbbec5a9b895ab2e99a3c300e3972348f53d9b941a1b
KBS	kbdNameService/KBDNameServiceLayout.sol	05db6bb2a6976409de2c62938ea7b7531b951fbde85395b38974351fe9df0c7f
KBL	kbdNameService/KBDNameServiceLogic.sol	a75c8c3bdf51321140217e9bbb67c7243a34983ec5f5ea2068d6359b8f898893
KBB	kbdNameService/KBDNameServiceLogicBase.sol	f33444d0fea8f35ec321fc7bcb49e0eb4eb3b00ab5aa811e5468299ff349cc51
KDN	kbdNameService/KBDNameServiceStorage.sol	840cd6f8794db50a14cea3fcd6f00db93bf25825e4e46b1919dd06558b5fbffe
KBT	kbdNameService/KBDNameServiceType.sol	e53c69d0dd943e765fb9ca3ee55ec9d12e646504fbc875819050162dc5594553
KBR	kbdNameServiceRef/KBDNameServiceRefEvent.sol	dbe2c18d83f311d6db712e64187b1aff52321efa18e19a327accfeba0061f914
KBI	kbdNameServiceRef/KBDNameServiceRefInterface.sol	2d4b491207bb0f03b05788f68d81bc6bd34f2b40d3b6b48158deb3a129cee2d0
KDS	kbdNameServiceRef/KBDNameServiceRefLayout.sol	ddaa0ef5967428f5c469eaee96f3a9385670dedd1f7c11ffd839a779cac8ca62
KDR	kbdNameServiceRef/KBDNameServiceRefLogic.sol	6a0665ce05de331e7b4c277b9095752f63aa55b7db4e784998af120af07ff782
KDL	kbdNameServiceRef/KBDNameServiceRefLogicBase.sol	af2e72a3af40dff3072afd30ff6c7d6364cf14cd6139f06181e15873649fab37
KNS	kbdNameServiceRef/KBDNameServiceRefStorage.sol	f834f4967c386be7babb1284a04205ec7ee55b047d8fd8c6ca92efc578e04b1a
KDT	kbdNameServiceRef/KBDNameServiceRefType.sol	d2fb327f095f75582f6bb36f49152e9c3fae3db195d3c6c238c0869a4562ed7f
KBE	manager/kbdManager/KBDManagerEvent.sol	6f2e008432f401f034236a3560cf44467681cae2f4cae127d3a0e74234d8dd98

ID	File	SHA256 Checksum
KDM	manager/kbdManager/KBDManagerInterface.sol	5f9ae0bc7006bd8a88b1fd2adae164ee8ad81702f4f86129cf3ac42d539403c5
KDI	manager/kbdManager/KBDManagerInterface1.sol	89b39d76f5718b7b25b0f3c8dacbfa6418d309274e652792853f95408960d3b3
KMI	manager/kbdManager/KBDManagerInterface2.sol	2c9524356c8094f27b20d1b81826d00d3ec9b7c3169fe0c1d7ed34421eaebf07
KBC	manager/kbdManager/KBDManagerInterfaceCommon.sol	8b61c4957fd0c0b986825fe29a3377fbd856df4558aedd1f61278d3222c6dcc1
KML	manager/kbdManager/KBDManagerLayout.sol	34b42de8520bb42cc9deb36c8b79b5b377cf9512d217c8d0ede426db2581e505
KMM	manager/kbdManager/KBDManagerLogic1.sol	9ef3ed49195ffeda10964d21a17ab62c7955d665f448fbf666abf55b6ad7c4c8
KLM	manager/kbdManager/KBDManagerLogic2.sol	07ec0032bb56c2042d0088fab91b1c97e7213e5c329bfc19ed7c3f4084c15f0b
KDB	manager/kbdManager/KBDManagerLogicBase.sol	e9d1277400f6fe112bfe15220ca914a9a7f7c54c697770cf9b6c66740ebefea7
KDC	manager/kbdManager/KBDManagerLogicCommon.sol	0e6d5419271df0cf86f75a7397ef3216dcbf496fd042ff01d5777c0564d0e78e
KMS	manager/kbdManager/KBDManagerStorage.sol	dc6b332c3bbdc1c31f1dd7db6e7890aeefecf0a6d0b8fd820730e4731c7be4e8
KMT	manager/kbdManager/KBDManagerType.sol	0db4534a1b0c2a1b43844cf8a5a75b2cf97fcca3331855ce5f6e58cd743d251c
KCR	nfts/kcard/KCARDEvent.sol	384588e04d0bd0f5863cf81f26a09b3b0e4de4f9eb1db975b15e6071ef977bb9
KCD	nfts/kcard/KCARDInterface.sol	98ff028eb2edcbd5012d75549c16e4269190c0d731c13a4ef4cf56184da4f9a6
KCL	nfts/kcard/KCARDLayout.sol	eab99c60bfb35e3ccd0e2306a8a3c703fcc6afc9598c87508c3829895c28a9c4
KAR	nfts/kcard/KCARDLogic.sol	8eebed5b9d2b32bb5df307a40d041e8356eddf57e2ab9f3cdd31efd572e121b9

ID	File	SHA256 Checksum
KCB	nfts/kcard/KCARDLogicBase.sol	4c8b0c290b0bd14d9299fb99ff1758a0239b23e87c0a5ece91a9298cf860da11
KCS	nfts/kcard/KCARDStorage.sol	9859eec07b3a7413058f3a2e188a47b8f873aa6d353869c31a5c7dbe99fa8e36
KCT	nfts/kcard/KCARDType.sol	99d102a78bb240617954e0b858b84ecb8d3df2de20c1a6947f3e9f363d0134f7
KDE	tokens/kbd/KBDEvent.sol	a0e8547a38a1c5ea6504c4cbe1b6fab4390b55fca59911e4ff69549734e8d5e7
BDI	tokens/kbd/KBDInterface.sol	0c1bfd433107ac8957ad61e10c7499abf92e953e81002e54cf1506751ce50a56
BDL	tokens/kbd/KBDLayout.sol	30601ff41c5ca0afceac9d9bc7c623c60480a1a5e15456ef57644cc7b25c21ea
KBG	tokens/kbd/KBDLogic.sol	82cfa845804aa37ca674fc151999e822fc7664085737cbeebb314066212e8b26
KLB	tokens/kbd/KBDLogicBase.sol	0a1842ef7ac9008644f5dbd87647c321fdc1a7b92eb8eeac35699d43cc3d8ae0
BDS	tokens/kbd/KBDStorage.sol	f20753f3a898b46e25dcdfd269eda4845d9fecb4f477bbee1ff3f7ce1eeddbde
BDT	tokens/kbd/KBDType.sol	bf849c61380a3a23700894d09e76a6babc62ecc057a9eab959a4ff8ad07de0ee
KGL	tokens/kgold/KGOLDEvent.sol	c9c1047e93296b32c59f8ad49a67767ecb68f2cd2f6c19920c2cd5677a1299f4
KGD	tokens/kgold/KGOLDInterface.sol	a4b450143ec2f85c4bf1f835ec83469f8824ae2ec1d20ed1af4006222bd13714
KOL	tokens/kgold/KGOLDLayout.sol	1514315e1bcba0710d7b94e73e95b272870e6b4dd954368c91e70196127a02ca
KOD	tokens/kgold/KGOLDLogic.sol	6955a1a8e1388e7bd409cacbb9333d60ddf72cac78addb6899171f9b3f07bd53
KGB	tokens/kgold/KGOLDLogicBase.sol	b30141f00aa1d66a196ad2a2605ddfcc907aa672c00c2c548a8495607eb6b824

ID	File	SHA256 Checksum
KGS	tokens/kgold/KGOLDStorage.sol	ef79be76b7259c69d512e863149019e46122a8af7365a162025f31e93790414d
KGT	tokens/kgold/KGOLDType.sol	6425d39103a07ab2c9f7011c4441c3977041be953f2a916442615c12e0a688d1

Findings



Critical	**0** (0.00%)
Major	**3** (42.86%)
Medium	**1** (14.29%)
Minor	**2** (28.57%)
Informational	**1** (14.29%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Require permission control in `mintSudo()` and `burnSudo()`	Control Flow	Minor	Resolved
GLOBAL-02	Centralization risk in proxy	**Centralization / Privilege, Logical Issue**	**Major**	Acknowledged
CON-01	Third party dependencies	Volatile Code	Medium	Acknowledged
CON-02	Missing emit events	Coding Style	Minor	Resolved
CON-03	Centralization related risks	**Centralization / Privilege**	**Major**	Acknowledged
HRM-01	Lack of token existence check	Volatile Code	Informational	Acknowledged
TOK-01	Logicacl issue of `mintSudo()` and `burnSudo()`	Control Flow	Major	Acknowledged

GLOBAL-01 | Require Permission Control In `mintSudo()` And `burnSudo()`

Category	Severity	Location	Status
Control Flow	Minor	Global	Resolved

Description

The functions `mintSudo()` and `burnSudo()` require permission contol. Although the contracts inherit `Proxy` contract and the permission control could be handled there, the proxy is not in the audit scope. The part is treated as a black box so it's not clear that if there is permission control in the two functions.

Recommendation

We recommend the team ensure the logic correctness.

Alleviation

The team heeded our advice and resolved the issue in commit 7cdae8bd2ecb30e5cbecdbbae61f2bd91bb26873.

GLOBAL-02 | Centralization Risk In Proxy

Category	Severity	Location	Status
Centralization / Privilege, Logical Issue	Major	Global	Acknowledged

Description

The contracts of the project are deployed with `proxy`. Apart from the logic in the specific logic contract, the contracts deployed via proxies can add additional permission controls or other logic. Since the proxy contract is not in the audit scope, it will be treated as a black box and assumed functional correctness. However, there will be potential centralization risk in the proxy:

- The admin of the proxy contract has the authority to execute any delegate call.

Any compromise to the `admin` account may allow the hacker to take advantage of this and users' assets may suffer loss.

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

The team acknowledged this issue and they will transfer the admin to dead address or Kyberdyne project owner when the project is stable.

CON-01 | Third Party Dependencies

Category	Severity	Location	Status
Volatile Code	Medium	depends/erc20improved/HERC20IMLogic.sol depends/erc721/HERC721Logic.sol tokens/kgold/KGOLDLogic.sol tokens/kbd/KBDLogic.sol nfts/kcard/KCARDLogic.sol	Acknowledged

Description

The contracts or modules `Ownable`, `AccessControl`, `Reentrancy`, `Proxy`, `Delegate`, `VRF`, `Deputy`, `NameService` and `HERC20` are not in the audit scope. The scope of the audit treats these contracts as black boxes and assumes their functional correctness.

The functions or modifiers involved are listed: `onlyOnce()`, `onlyOwner()`, `ac.isBlocked()`, `ac.isPrivileged()`, etc.

Recommendation

We understand that the business logic of the project requires interaction with those contracts. We encourage the team to ensure their functional correctness.

Alleviation

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

CON-02 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Minor	depends/erc20improved/HERC20IMLogic.sol depends/erc721/HERC721Logic.sol tokens/kbd/KBDLogic.sol tokens/kgold/KGOLDLogic.sol nfts/kcard/KCARDLogic.sol	Resolved

Description

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

In the contract `HERC20IMLogic`,

- `setAccessControl()`
- `setSupport()`

AND

In the contract `HERC721IMLogic`,

- `setAccessControl()`
- `setSupport()`

AND

In the contract `KBDLogic`,

- `mintSudo()`
- `burnSudo`

AND

In the contract `KGOLDLogic`,

- `mintSudo()`
- `burnSudo`

AND

In the contract `KCARDLogic`,

- `mintSudo()`

- `burnSudo()`
- `setUint256Attribute()`
- `setBytes32Attribute()`
- `setAddressAttribute()`
- `setBytesAttribute()`

Recommendation

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

```
    event SetAccessControl(address accessControl);
    function setAccessControl(address accessControl_) override external onlyOwner {
        _setAccessControl(accessControl_);
        emit SetAccessControl(accessControl_);
    }
```

Alleviation

The team fixed the issue in commit 7cdae8bd2ecb30e5cbecdbbae61f2bd91bb26873 and ec71cd891a57d5b00608837bd1b46dccfc9797c9.

CON-03 | Centralization Related Risks

Category	Severity	Location	Status
Centralization / Privilege	**Major**	depends/erc20improved/HERC20IMLogic.sol depends/erc721/HERC721Logic.sol nfts/kcard/KCARDLogic.sol	Acknowledged

Description

In the contract `HERC20IMLogic`, the role `owner` has authority over the following functions:

- function setAccessControl(), set value for accessControl.
- function setSupport(), set value for support.

AND

In the contract `HERC721IMLogic`, the role `owner` has authority over the following functions:

- function setAccessControl(), set value for accessControl.
- function setSupport(), set value for support.

AND

In the contract `KCARDLogic`, the role `owner`, `manager` or `operator` has the authority over the following functions:

- function mintSudo(), mint tokens for any arbitrary address.
- function bind() and unbind(), manage the relationship between offline id and token id.
- function burnSudo(), burn token from any arbitrary address.
- function setUint256Attribute(), set attributes for the token.
- function setBytes32Attribute(), set attributes for the token.
- function setAddressAttribute(), set attributes for the token.
- function setBytesAttribute(), set attributes for the token.

Any compromise to the privileged accounts may allow a hacker to take advantage of this authority and bring unpredicatable damages to the project.

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 this issue and they will transfer the admin roles to dead address or Kyberdyne project owner when the project is stable.

HRM-01 | Lack Of Token Existence Check

Category	Severity	Location	Status
Volatile Code	Informational	depends/erc721improved/HERC721IMLogic.sol: 40, 60	Acknowledged

Description

The functions `_mintSudo()` and `_mintNormal()` lack the check `!_exists(tokenId)`.

Recommendation

We recommend the team add the check in the two functions like that in the function `_burnNormal()` and `_burnSudo()`.

Alleviation

The team stated that the existence check has been done in the contract `HERC721Logic`.

TOK-01 | Logicacl Issue Of `mintSudo()` And `burnSudo()`

Category	Severity	Location	Status
Control Flow	Major	tokens/kgold/KGOLDLogic.sol tokens/kbd/KBDLogic.sol	Acknowledged

Description

The functions `mintSudo()` and `burnSudo()` can mint tokens for arbitrary address. Especially `burnSudo()` allows the caller to burn money from any user's wallet. Usual tokens don't have the function or require allowance to perform the burn operation. There are high risks in the user's property security.

Recommendation

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

Alleviation

The team acknowledged this issue and they stated the following:

"The KBD is minted up to the cap so the mintSudo and burnSudo function is useless. The admin of KBD will transfer to dead address once online. The KGOLD will be minted on demand due to offline game server. The admin of KGOLD will be set to offline server's address."

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.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

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.