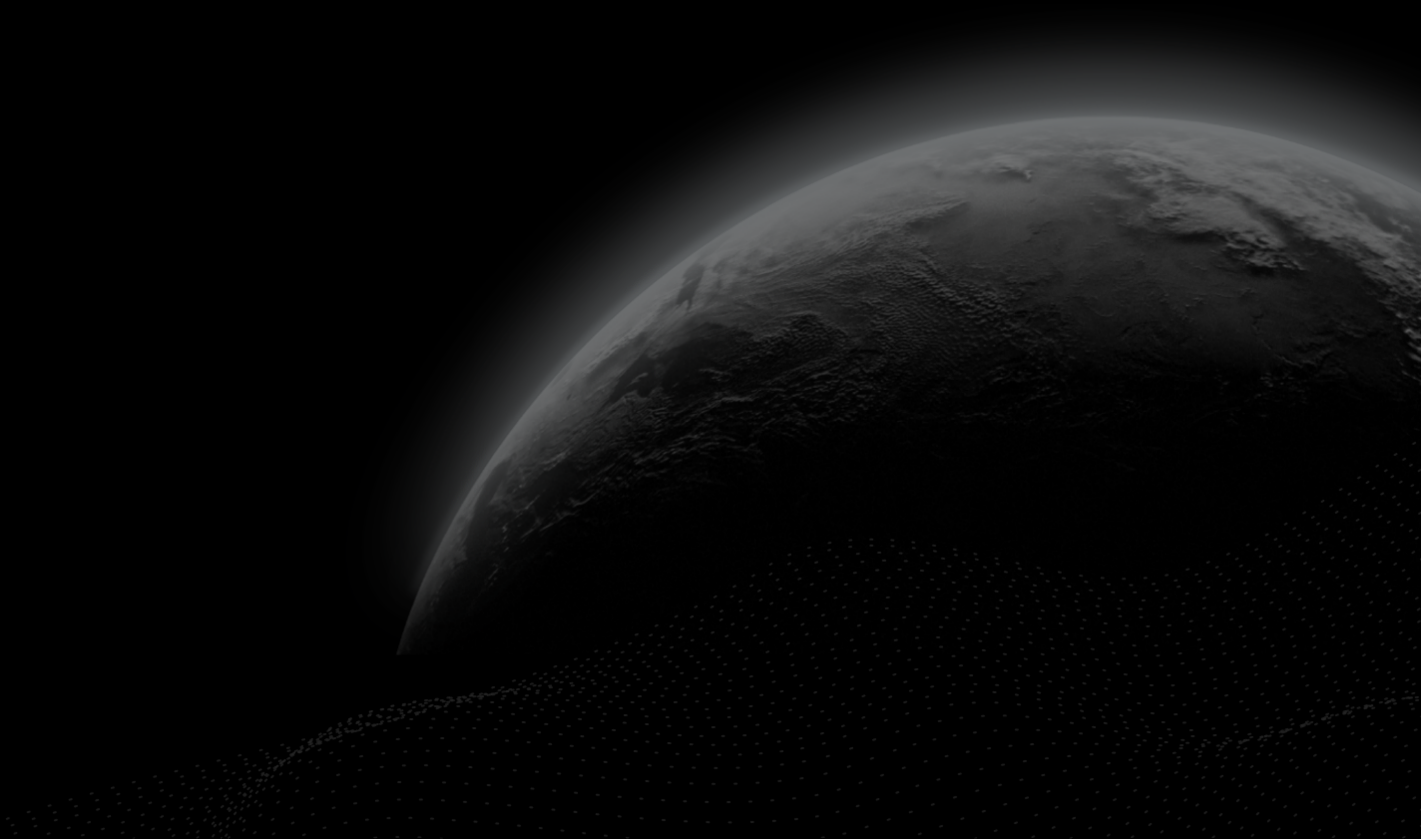
CERTIK

Security Assessment

UBOX-NFT DEX

CertiK Assessed on Nov 28th, 2023



CertiK Assessed on Nov 28th, 2023

UBOX-NFT DEX

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Ethereum (ETH)	Manual Review, Static Analysis

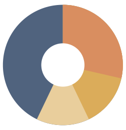
LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 11/28/2023	N/A

CODEBASE

Private Repository

View All in Codebase Page

Vulnerability Summary



7	5	0	0	2	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

🟥 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.
🟧 2	Major	2 Acknowledged	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.
🟨 1	Medium	1 Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨 1	Minor	1 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 | UBOX-NFT DEX

Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Review Notes

Findings

EOS-01 : Centralization Risks

UNT-02 : Centralized Control of Contract Upgrade

UNT-01 : Potential Damage Due to Unprotected Initializer

UNT-03 : Ineffective Use of Reentrancy Guard

EOS-02 : Missing Emit Events

UNT-04 : Manager should ensure the contract balance enough for redeem

UNT-05 : Lack of Storage Gap in Upgradeable Contract

Appendix

Disclaimer

CODEBASE | UBOX-NFT DEX

Repository

Private Repository

AUDIT SCOPE | UBOX-NFT DEX

47 files audited ● 2 files with Acknowledged findings ● 45 files without findings

ID	Repo	File	SHA256 Checksum
● UNF	CertiKProject/certik-audit-projects	eosmint-20231120/UboxNFT1155.sol	15b6bc2fd3e036cd3733118f5fc725883b2517ad8bbc21e7c393bfa2d9906d74
● UNT	CertiKProject/certik-audit-projects	eosmint-20231120/UboxNFT1155Store.sol	a5973b7c656511a5b1eec889be7bd9140ccb1ee7ce6298bde2bc9eed07de73ca
● IBE	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IBasicERC721OrdersFeature.sol	5dcf74c2c2987f90e17e0d5077c3d84a68eaa05028d88184c3c5e758ce9b780c
● IBS	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IBatchSignedERC721OrdersFeature.sol	cf3e0e1e996ed40cc454e2b81de94833a3683ca43655376add051955189f8df5
● IBF	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IBootstrapFeature.sol	f526d603388a50719e583032e4d5be2fcac93e5781c495a709127ac453a39891
● IER	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IERC1155OrdersEvent.sol	b295a86ad83aa81f6a21ffc9a0d4fe71948a0861702bf0f53b57219d26fcf3dd
● IEC	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IERC1155OrdersFeature.sol	97e437dd0679473ea07e00f2cccafe3576eabf66eb8129cfe93ad0e880a36145
● IEO	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IERC721OrdersFeature.sol	6395d20e1df68128afa6d8e3167219028931e57271d9cd1c5a88fcbf5b96cf5c
● IFE	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IFeature.sol	4f59fec73c55ecf258f2b0a8bed9feecb88aab365df9ae8cdaa3aa1cc95cc8b0
● INF	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/INFTOrdersFeature.sol	e942d684d32fbc1ce1fa8ef487163eb7e7fe1c2fee0dd858cbc4658ee9a8cb31
● INT	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/INFTransfersFeature.sol	597e711b0c0bd5c9d0c3ef02d0f57040d70574fbaae7ee943fffb1a5866d65a3
● IOF	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/IOwnableFeature.sol	0af3264b95c77a866eea69c86784a92ed1805269a1fa16a11124f0ed0575bcf4
● ISF	CertiKProject/certik-audit-projects	uboxEX/features/interfaces/ISimpleFunctionRegistryFeature.sol	976f4beaa41b709865987908d6f06b596d619c556088a3dcdb607fd2c6b102e4

ID	Repo	File	SHA256 Checksum
LNF	CertiKProject/certik-audit-projects	uboxEX/features/libs/LibNFTOrder.sol	e84a0b2f8c3bd962f986a89d3243a0885a4a48587ac1fb7e069c731f1c1cefea
LSE	CertiKProject/certik-audit-projects	uboxEX/features/libs/LibSignature.sol	3892a39f7f290bd382a2fe34e3b875d404f908b826a0432b16c729b8c4d13d61
RGE	CertiKProject/certik-audit-projects	uboxEX/features/libs/ReentrancyGuard.sol	d69f98399d8592250cca5e10bdbd6d7d1aa21f5b4fdac8491a86f033d1ba3445
BER	CertiKProject/certik-audit-projects	uboxEX/features/nft_orders/BasicERC721OrdersFeature.sol	f50e724b23d6fadb523939d0b48f9c02c7864bb2eae0aa6a768d91b4074b974f
BSE	CertiKProject/certik-audit-projects	uboxEX/features/nft_orders/BatchSignedERC721OrdersFeature.sol	f5a97111d849678414ea0b3568aee7fad639a36d9ebfe821a50c589ca59d59ef
ERC	CertiKProject/certik-audit-projects	uboxEX/features/nft_orders/ERC1155OrdersFeature.sol	9459b119ca38234b0478cbeeceafbff29c6947f1f6cf6b80926cf5c2239dbc40
ERO	CertiKProject/certik-audit-projects	uboxEX/features/nft_orders/ERC721OrdersFeature.sol	aa0e539051c141fe6213dd77cc6eaeac4e75178f7f53e61b2b6a1d24cb8b6342
NFT	CertiKProject/certik-audit-projects	uboxEX/features/nft_orders/NFTOrders.sol	d243a74fb9f3c050d025babfa10e6f5dae1cc1db25bdd78b415bcdf60a6af4c6
NFF	CertiKProject/certik-audit-projects	uboxEX/features/nft_transfers/NFTransfersFeature.sol	7d05ed7e9b40d23bb69e5f08232d99f12e10ceac359cdb5633b420a35a9379e0
BFE	CertiKProject/certik-audit-projects	uboxEX/features/BootstrapFeature.sol	20548827ceb9c53af621618e5ddcfc6ab8937d2d4c74e3f030f80d6e2cf7b8a8
OFE	CertiKProject/certik-audit-projects	uboxEX/features/OwnableFeature.sol	0a86394368772ed96bef0cd5fc4761102e17a7ce7010dd0f93d2f44c6f4cb1ff
SFR	CertiKProject/certik-audit-projects	uboxEX/features/SimpleFunctionRegistryFeature.sol	ca1788bb046bf30f72a30d8132fba925f695a05efa57e579541bdcae0b327aaf
FCE	CertiKProject/certik-audit-projects	uboxEX/fixins/FixinCommon.sol	18a2dd544180922c38cca4145bff7e86dd9d3f0f496956bcda3654065540ca13
FEI	CertiKProject/certik-audit-projects	uboxEX/fixins/FixinEIP712.sol	d2ede85cee456f61a484d8f47bf82d7b322a1b56c14b8eeebf67574fa886ab2c
FER	CertiKProject/certik-audit-projects	uboxEX/fixins/FixinERC1155Spender.sol	401e352900eb85dd8383019e4d1d211c8de4255cb3c032379e95dfff564a54e5

ID	Repo	File	SHA256 Checksum
FEC	CertiKProject/certik-audit-projects	uboxEX/fixins/FixinERC721Spender.sol	a0c2e5e8d18a34b0cdf1797488b27d3e18d0fe1fa65fc6dde95d48527dedeafa
FTS	CertiKProject/certik-audit-projects	uboxEX/fixins/FixinTokenSpender.sol	0b9841738d202f92462f1fdd7a1460216b6e32ce581414061c24ca284aa84e12
IME	CertiKProject/certik-audit-projects	uboxEX/migrations/InitialMigration.sol	0a4fe9858b010c70725672e9cd0d760d972950edca8635d61b40892ac222a608
LBE	CertiKProject/certik-audit-projects	uboxEX/migrations/LibBootstrap.sol	ad1d41a0407abae1279328a67fb51b226dfd92cc10273ea4c7eff9300d499e5b
LME	CertiKProject/certik-audit-projects	uboxEX/migrations/LibMigrate.sol	d2a2ee5746797d43f52e68bcf70d953776e6d1e675f0bab637a56c7096ce5841
LCN	CertiKProject/certik-audit-projects	uboxEX/storage/LibCommonNftOrdersStorage.sol	683fce8953dff837f74f2cabd1f316fca194e887eb89b72bd8a2ab0719e28ee3
LER	CertiKProject/certik-audit-projects	uboxEX/storage/LibERC1155OrdersStorage.sol	f3619ff0250b1d1489169fdba8e9de4af4ec15dd911f57dc17a77c61ca62ad1d
LEC	CertiKProject/certik-audit-projects	uboxEX/storage/LibERC721OrdersStorage.sol	2ba2659d0fbf0a70c5c3dba2c49260b76288fb6c0ece70b91d40595cedd5997a
LHF	CertiKProject/certik-audit-projects	uboxEX/storage/LibHelperFeatureStorage.sol	c3d2ebdf585037b60ae0ed5bb58034a31cb69f8930d54841f2c47bdc7c087c4a
LHS	CertiKProject/certik-audit-projects	uboxEX/storage/LibHelperStorage.sol	78989ef5eca42ae4e2573c44ac397eaa2d1cd2b237846040fe856efa115fcd41
LOS	CertiKProject/certik-audit-projects	uboxEX/storage/LibOwnableStorage.sol	6e907d5d769b56382431845d86c12eb83ba3698d3403607ca6e134c2b68458e0
LPS	CertiKProject/certik-audit-projects	uboxEX/storage/LibProxyStorage.sol	44cbf6c78229433151b876bb611a0bcd96330d24f65a3cd69a3c56ceec2e0493
LSF	CertiKProject/certik-audit-projects	uboxEX/storage/LibSimpleFunctionRegistryStorage.sol	6f2996bce8d9ff2160181da0a295c550f139e22a4ce2f81b2b5cb83790655b7b
LSX	CertiKProject/certik-audit-projects	uboxEX/storage/LibStorage.sol	2c93059671afaaf8f758dc6db7589f7db54d28c71ba61edd9c0c855168431754
IET	CertiKProject/certik-audit-projects	uboxEX/vendor/IEtherToken.sol	c39c4515c6bc6d43ba59adfd6d988d57e85a525074181a378ac79ba33cbd2f29

ID	Repo	File	SHA256 Checksum
IFR	CertiKProject/certik-audit-projects	uboxEX/vendor/IFeeRecipient.sol	5102748ee834442457d0f96ea6aaccf76ff7612fa193413605d360c6345da9db
IPV	CertiKProject/certik-audit-projects	uboxEX/vendor/IPropertyValidator.sol	8fba7b3aabbcf5deac91c038205b63f396060b7eb0df1a683fdfd106b7155be1
ITC	CertiKProject/certik-audit-projects	uboxEX/vendor/ITakerCallback.sol	82669eea30715c6677907b17cd636d6bd2858a70da17320c6d1b1f4b459e2cd3
UBE	CertiKProject/certik-audit-projects	uboxEX/UBoxEx.sol	4d121a82f189167adabc99fe71d3bdd9a141e9941010ca330e86c66fb0750c14

APPROACH & METHODS | UBOX-NFT DEX

This report has been prepared for UBOX-NFT to discover issues and vulnerabilities in the source code of the UBOX-NFT DEX project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

REVIEW NOTES | UBOX-NFT DEX

The Ubox-NFT DEX smart contracts are designed as a marketplace for trading NFTs, specifically catering to users in the Asia-Pacific region.

The scope of the audit consists of two parts:

1. Verify that the Ubox-EX contracts are forked from element-market, and this part of the audit focused solely on the differences between the original `element-market` contracts and the `Ubox` contracts.
2. Full audit to two `eosmint` contracts: UboxNFT1155.sol and UboxNFT1155Store.sol.

FINDINGS | UBOX-NFT DEX

Total Findings	Critical	Major	Medium	Minor	Informational
7	0	2	1	1	3

This report has been prepared to discover issues and vulnerabilities for UBOX-NFT DEX. Through this audit, we have uncovered 7 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
EOS-01	**Centralization Risks**	**Centralization**	**Major**	● **Acknowledged**
UNT-02	**Centralized Control Of Contract Upgrade**	**Centralization**	**Major**	● **Acknowledged**
UNT-01	Potential Damage Due To Unprotected Initializer	Logical Issue	Medium	● Resolved
UNT-03	Ineffective Use Of Reentrancy Guard	Concurrency	Minor	● Resolved
EOS-02	Missing Emit Events	Coding Style	Informational	● Resolved
UNT-04	Manager Should Ensure The Contract Balance Enough For Redeem	Logical Issue	Informational	● Resolved
UNT-05	Lack Of Storage Gap In Upgradeable Contract	Design Issue	Informational	● Resolved

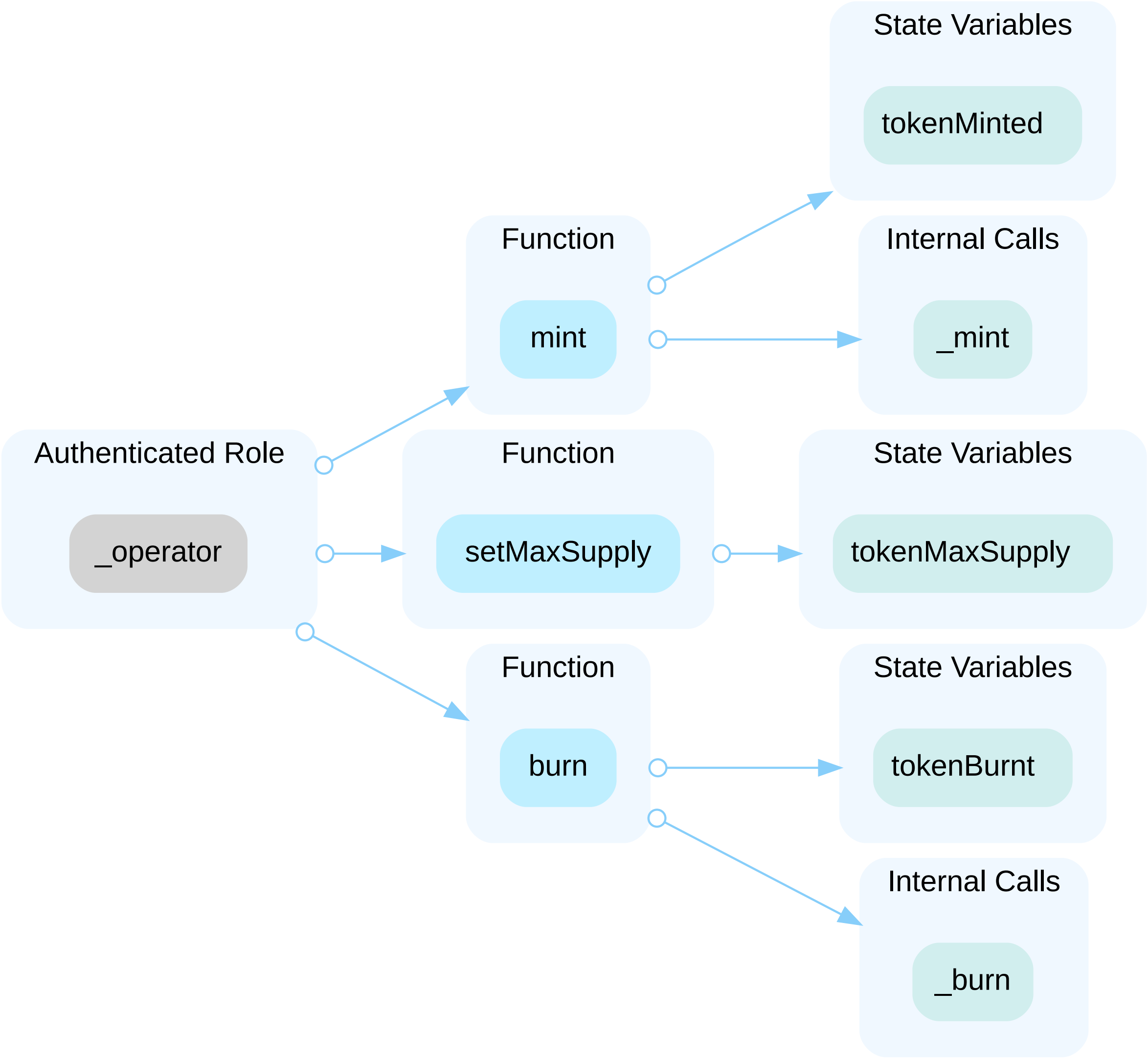
EOS-01 | CENTRALIZATION RISKS

Category	Severity	Location	Status
Centralization	● Major	eosmint-20231120/UboxNFT1155.sol (eosmint): 29, 33, 38, 43, 48, 56; eosmint-20231120/UboxNFT1155Store.sol (eosmint): 107, 111, 115, 119, 123, 128, 133, 138, 147	● Acknowledged

Description

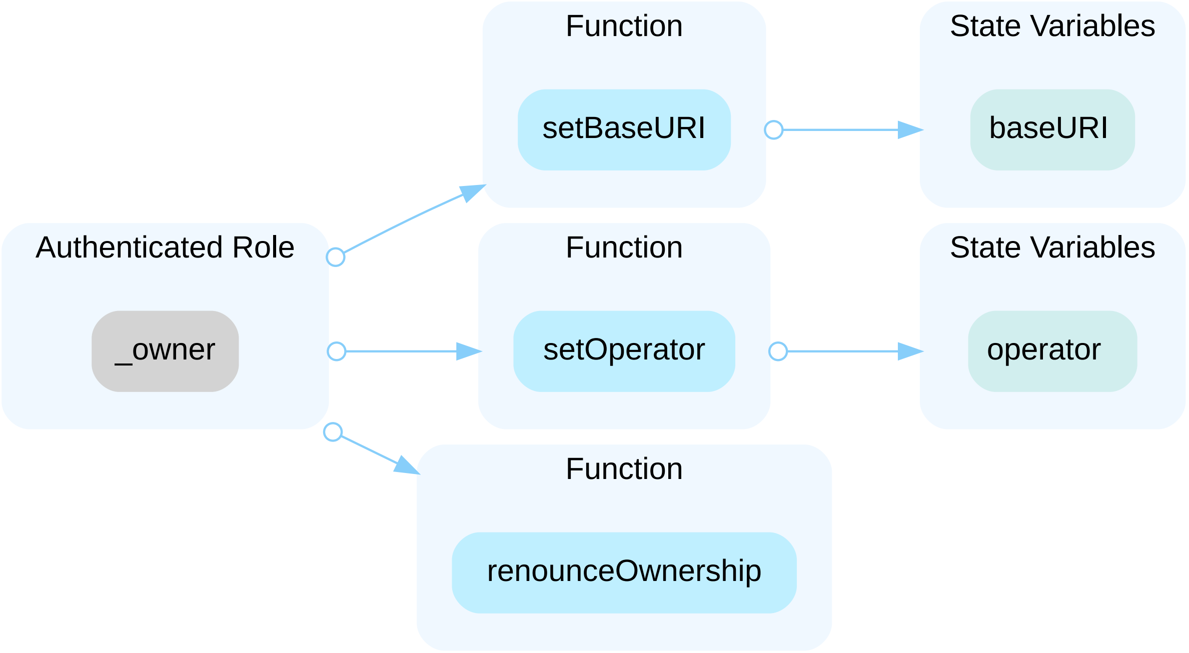
In the contract `UboxNFT1155` the role `_operator` has authority over the functions shown in the diagram below. Any compromise to the `_operator` account may allow the hacker to take advantage of this authority and:

- set the max supply of certain `_tokenId` ,
- mint any amount of tokens for any `_tokenId` to any address,
- burn tokens for any `_tokenId` from the caller;



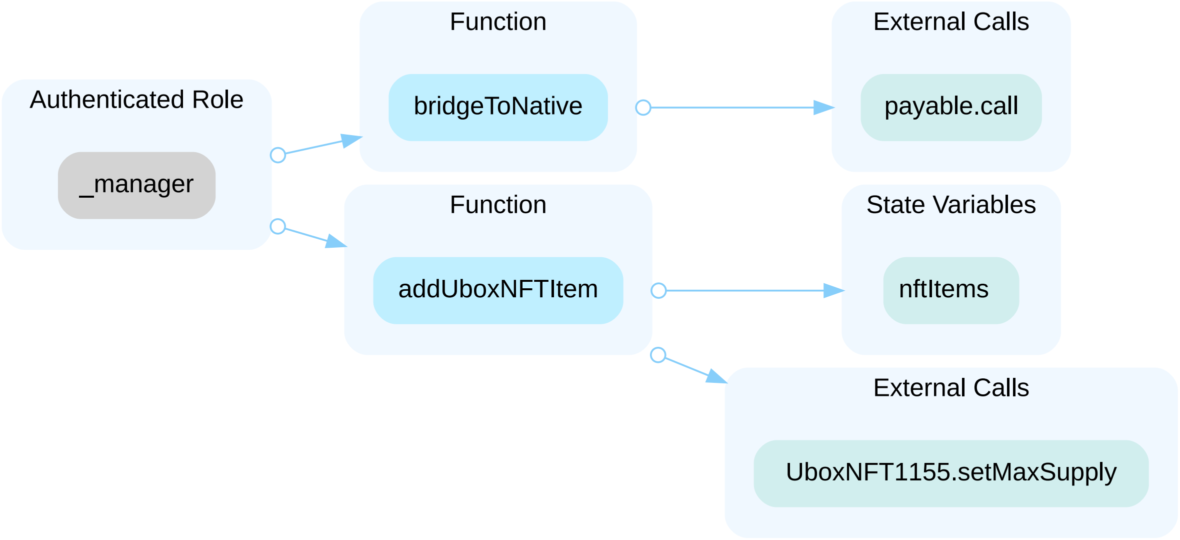
In the contract `UboxNFT1155` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and:

- set the operator address,
- set BaseURI of the ERC1155;



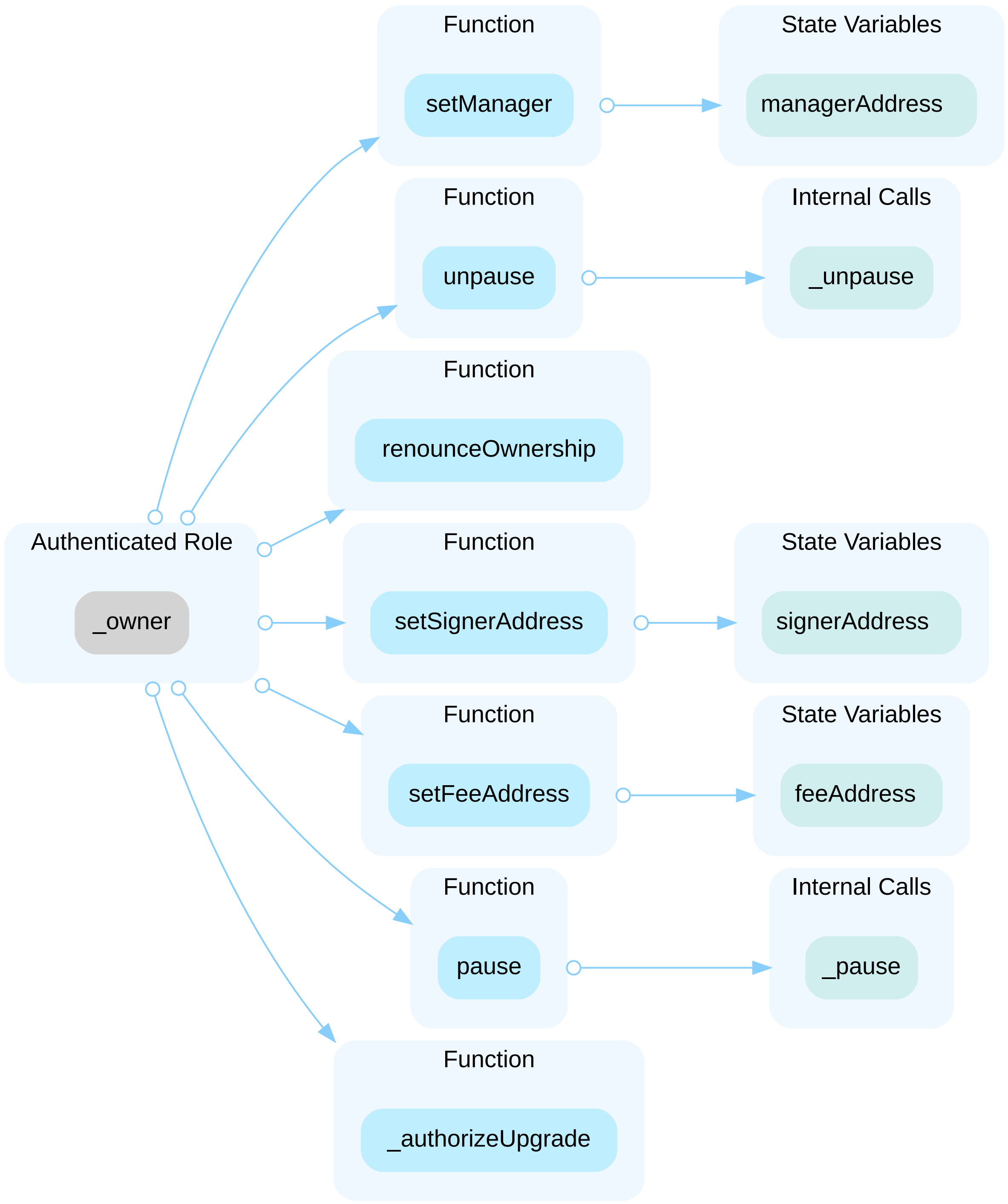
In the contract `UboxNFT1155Store` the role `_manager` has authority over the functions shown in the diagram below. Any compromise to the `_manager` account may allow the hacker to take advantage of this authority and:

- add ubox nft item: set max supply for certain `_tokenId` ,
- extract all platform native tokens from the contract to the bridge address;



In the contract `UboxNFT1155Store` 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:

- upgrade the contract implementation,
- pause,unpause the contract,
- set feeAddress/managerAddress/signerAddress;



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

[UBOX-NFT DEX, 11/23/2023]:

The `_operator` in UboxNFT1155 will be set to the UboxNFT1155Store contract address. Both minting and burning will go through validation by the UboxNFT1155Store. The `_owner` and `_manager` in UboxNFT1155Store will be modified to a Timelock contract address within one week after contract deployment.

UNT-02 | CENTRALIZED CONTROL OF CONTRACT UPGRADE

Category	Severity	Location	Status
Centralization	● **Major**	**eosmint-20231120/UboxNFT1155Store.sol (eosmint): 16**	● **Acknowledged**

Description

In the contract UboxNFT1155Store, the role `owner` has the authority to update the implementation contract behind the UboxNFT1155Store contract.

Any compromise to the `owner` account may allow a hacker to take advantage of this authority and change the implementation contract which is pointed by proxy and therefore execute potential malicious functionality in the implementation contract.

Recommendation

We recommend that the team make efforts to restrict access to the admin of the proxy contract. A strategy of combining a time-lock and a multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. In addition, the team should be transparent and notify the community in advance whenever they plan to migrate to a new implementation contract.

Here are some feasible short-term and long-term suggestions that would mitigate the potential risk to a different level and suggestions that would permanently fully resolve the risk.

Short Term:

A combination of a time-lock and a multi signature (⅔, ⅗) wallet mitigate the risk by delaying the sensitive operation and avoiding a single point of key management failure.

- A time-lock with reasonable latency, such as 48 hours, for awareness of privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to a private key compromised;
  AND
- A medium/blog link for sharing the time-lock contract and multi-signers addresses information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.
- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.

- Provide a link to the **medium/blog** with all of the above information included.

Long Term:

A combination of a time-lock on the contract upgrade operation and a DAO for controlling the upgrade operation mitigate the contract upgrade risk by applying transparency and decentralization.

- A time-lock with reasonable latency, such as 48 hours, for community awareness of privileged operations;
  AND
- Introduction of a DAO, governance, or voting module to increase decentralization, transparency, and user involvement;
  AND
- A medium/blog link for sharing the time-lock contract, multi-signers addresses, and DAO information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.
- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.
- Provide a link to the **medium/blog** with all of the above information included.

Permanent:

Renouncing ownership of the `admin` account or removing the upgrade functionality can *fully* resolve the risk.

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

Alleviation

[UBOX-NFT DEX, 11/23/2023]: The `_owner` in UboxNFT1155Store will be modified to a Timelock contract address within one week after contract deployment.

UNT-01 | POTENTIAL DAMAGE DUE TO UNPROTECTED INITIALIZER

Category	Severity	Location	Status
Logical Issue	● Medium	eosmint-20231120/UboxNFT1155Store.sol (eosmint): 86	● Resolved

Description

One or more logic contracts do not protect their initializers. An attacker can call the initializer and assume ownership of the logic contract, whereby she can perform privilelged operations that either indirectly break the proxy by destroying the logic contract or trick unsuspecting users into believing that she is the owner of the upgradeable contract.

```
16  contract UboxNFT1155Store is
```

- `UboxNFT1155Store` is an upgradeable contract that does not protect its initializer.

```
86      function initialize(
```

- `initialize` is an unprotected initializer function.

Recommendation

It is advised to call `_disableInitializers` in the constructor or give the constructor the initializer modifier to prevent the intializer from being called on the logic contract.

Reference: https://docs.openzeppelin.com/upgrades-plugins/1.x/writing-upgradeable#initializing_the_implementation_contract

Alleviation

The team heeded our advice and resolved the issue in the latest version by adding the below code.

```
    /// @custom:oz-upgrades-unsafe-allow constructor
    constructor() {
        _disableInitializers();
    }
```

The sha256 checksum of UboxNFT1155Store.sol is b922729b2548643d98c4446cc34f3d5d6efa14803baa434784a58b25131a2b72.

UNT-03 | INEFFECTIVE USE OF REENTRANCY GUARD

Category	Severity	Location	Status
Concurrency	● Minor	eosmint-20231120/UboxNFT1155Store.sol (eosmint): 153~210	● Resolved

Description

In `UboxNFT1155Store.sol` , the reentrancy guard `nonReentrant` is applied to function `redeem()` . Applying the `nonReentrant` modifier to only one of the user-facing functions limits its effectiveness and use as reentrancy protection. This only prevents reentrancy that starts and iterates through function `redeem()` and does not prevent cross-function reentrancy that may start in other functions and reenter through `redeem()` , or start in `redeem()` and reenter through other functions. The following user-facing, state-changing functions remain open to potential cross-function reentrancy combinations:

- `mint()`

Adding a `nonReentrant` modifier to the functions above will increase the effectiveness of the reentrancy guard.

Recommendation

We recommend adding the `nonReentrant` modifier where specified.

Alleviation

The team heeded our advice and resolved the issue in the latest version by adding the `nonReentrant` modifier to the `mint()` function.

The sha256 checksum of UboxNFT1155Store.sol is b922729b2548643d98c4446cc34f3d5d6efa14803baa434784a58b25131a2b72.

EOS-02 | MISSING EMIT EVENTS

Category	Severity	Location	Status
Coding Style	● Informational	eosmint-20231120/UboxNFT1155.sol (eosmint): 29~31, 33~36, 38~41, 43~46, 48~54, 56~61; eosmint-20231120/UboxNFT1155Store.sol (eosmint): 107, 111~113, 115~117, 119~121, 123~126, 128~131, 133~136, 138~145, 147~151	● Resolved

Description

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

Recommendation

It is recommended to emit events in sensitive functions that are controlled by centralization roles.

Alleviation

The team heeded our advice and resolved the issue in the latest version.

The sha256 checksum of UboxNFT1155Store.sol is b922729b2548643d98c4446cc34f3d5d6efa14803baa434784a58b25131a2b72.

UNT-04 | MANAGER SHOULD ENSURE THE CONTRACT BALANCE ENOUGH FOR REDEEM

Category	Severity	Location	Status
Logical Issue	● Informational	eosmint-20231120/UboxNFT1155Store.sol (eosmint)	● Resolved

Description

Since the manager can transfer the contract balance to the bridge address, and fee will be transferred to the fee address during mint, the contract balance could be not enough when users redeem.

Recommendation

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

Alleviation

[UBOX-NFT DEX, 11/23/2023]: We will monitor the contract's balance. If it is insufficient, we will manually add more funds to it.

UNT-05 | LACK OF STORAGE GAP IN UPGRADEABLE CONTRACT

Category	Severity	Location	Status
Design Issue	● Informational	eosmint-20231120/UboxNFT1155Store.sol (eosmint): 17~18	● Resolved

Description

There is no storage gap preserved in the logic contract. Any logic contract that acts as a base contract that needs to be inherited by other upgradeable child should have a reasonable size of storage gap preserved for the new state variable introduced by the future upgrades.

Recommendation

We recommend having a storage gap of a reasonable size preserved in the logic contract in case that new state variables are introduced in future upgrades. For more information, please refer to: https://docs.openzeppelin.com/contracts/3.x/upgradeable#storage_gaps.

Alleviation

The team heeded our advice and resolved the issue in the latest version by adding the storage gap.

The sha256 checksum of UboxNFT1155Store.sol is b922729b2548643d98c4446cc34f3d5d6efa14803baa434784a58b25131a2b72.

APPENDIX | UBOX-NFT DEX

Finding Categories

Categories	Description
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
Concurrency	Concurrency findings are about issues that cause unexpected or unsafe interleaving of code executions.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

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.